DESIGN AND ANALYSIS OF VARIOUS SENSORS FOR ELECTROMAGNETIC SIDE CHANNEL RECEPTION

A Dissertation
Presented to
The Academic Faculty

by

Sinan Adibelli

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Electrical and Computer Engineering

Georgia Institute of Technology
December 2020

DESIGN AND ANALYSIS OF VARIOUS SENSORS FOR ELECTROMAGNETIC SIDE CHANNEL RECEPTION

Approved by:

Dr. Alenka Zajic, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Milos Prvulovic
School of Computer Science
Georgia Institute of Technology

Dr. Andrew Peterson
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Hua Wang
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Gregory David Durgin
School of Electrical and Computer Engineering
Georgia Institute of Technology

Date Approved: [October 23, 2020]

ACKNOWLEDGEMENTS

I would like to thank my supervisor Prof. Alenka Zajic for her guidance and support during this research. I sincerely feel fortunate to have joined this lab. Moreover, I would like to thank Prof. Andrew Peterson, Prof. Gregory Durgin, Prof. Milos Prvulovic, Prof. Hua Wang for their feedback on my documents and appearing on my thesis committee. Additionally, I would like to thank Dr. Prateek Juyal for keeping me motivated to complete my tasks without delay.

I would like to thank my parents Zehra Adibelli and Hamit Adibelli for supporting me throughout my education. I also thank my cousin Dincer Unluer for his guidance and initially motivating me to pursue a doctorate here. Finally, I would like to thank my friends in the US and Turkey for their support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

The objective of the presented research is to design and analyze electromagnetic (EM) sensors such as antennas, near field probes, and near field focusers for the application of detecting electromagnetic side channel signals directly or through backscattering.

EM side channels are unintentional electromagnetic emanations produced by digital circuits as they perform their intended function. This thesis focuses on detecting unintentional electromagnetic emanations that are produced by computer systems such as processors, embedded devices, FPGAs, integrated circuits (ICs), etc. Side channel detection is difficult due to the mechanism of radiation being an unintentional source of signals. To detect them, there are particular requirements of an EM sensor such as resolution, gain, sensitivity, frequency response, and backscattering schemes.

To enable detection of side channel signals from 1 GHz to 300 GHz in the near field and the far field, this thesis proposes an easily scalable panel antenna with high gain, a high resolution E and H probe pair intended to be used in a backscattering setup, a THz near field reflector focuser, utilization of polarization filtering techniques, and THz far field reflectors. Each of these designs is first analyzed individually, then evaluated in the context of its intended application and finally its efficiency was validated in its intended application.

This thesis provides other researchers with guidelines on how to select and design electromagnetic sensors for side channel detection as well as develop further understanding of the interaction between these electromagnetic sensors and side channels.

CHAPTER 1. INTRODUCTION

1.1 Motivation and Overview

Any analog signal created by a computer system as an unintended side effect of performing a computation is called an analog side channel. Analog side channels appear in many forms including fluctuations in power consumption, acoustic noises, cache accesses, and most importantly electromagnetic emanations, which is what this thesis focuses on. Electromagnetic side channels have the particular benefit of being detectable at a distance and being able to make use of modulation, which makes it possible to receive electromagnetic side channels at many widely different frequency bands as well as allowing for backscattering schemes to be used [1]. These techniques are relevant in the field of hardware security because they can be used to steal cryptographic keys as well as monitor for and detect malicious modifications in computer systems.

However, due to the fact that electromagnetic side channels are created unintentionally as a side effect of the physical implementation of the intended behavior, the power levels are very low, and detection is difficult. Previously, standard commercial antennas and commercial near field probes have been used to measure EM side channels, but it is possible to improve the performance of the side channel analysis techniques by deliberately designing the EM sensing structures. The applications we are interested in have specific requirements in terms of frequency, noise characteristics, gain, spatial resolution, sensitivity, and size. Hence, this thesis focuses on a careful evaluation of the tradeoffs between the relevant quantities.

In order to improve the effectiveness of EM side channel techniques, we study the design and analysis of a high gain easily scalable microwave far field antenna, a high resolution microwave E and H field probe pair for backscattering measurements, a THz near field focuser, a THz backscattering scheme that exploits polarization effects, and a THz reflector to extend the range of these techniques; all of which take into consideration the specific requirements of the application in order to achieve optimal performance along with a demonstration of its performance in that associated application.

In addition to the design and analysis of the aforementioned EM sensors on their own and in application, we propose an analysis of some of the underlying phenomenon such as the noise behavior with respect to distance and the unintentional backscattering from ICs that will provide a deeper understanding of side channels and backscattered side channels from an EM point of view.

First, we will introduce the current state of the research areas that are addressed in Chapters 3 through 6 and summarize the contributions of this thesis.

1.2 Electromagnetic Side Channels and Detection at a Distance

To perform computational tasks, integrated circuits (ICs), such as processors and FPGAs, leverage electrical and architectural complexity. In doing so, many unintentional effects such as power fluctuations, cache accesses, acoustic noise, and electromagnetic radiation can be triggered. Signals coming from these processes can be detected and be used to make deductions regarding what kind of computation is being performed [2].

This thesis is only interested in EM side channels. Almost any computational activity results in a change in current, which results in EM radiation. Components in these systems create emanations due to current changes related to their primary function along with current changes related to nearby components as a result of coupling and circuit geometry. Data processing is the most common type of activity to be targeted using EM side channels [3].

Emanations caused by data processing operations have been exploited heavily through side channel analysis for the purpose of data theft, stealing cryptographic keys and breaking encryption. Due to the complexity of computer systems, physical implementation of encryption algorithms trigger many side effects in addition to the desired I/O information [4]. Side channel attacks are able to get around widely used security measures by exploiting the measurable side effects of the algorithm rather than trying to access the direct functionality of the algorithm.

However, the uses of side channel analysis are not restricted to malicious purposes. Side channels have been shown to be effective in spotting malicious behavior in software (e.g. detecting malware [2], [5]) and in hardware (e.g. Trojan detection [6], [7]). Recently, side channels have been used in a new backscattering scheme to detect Hardware Trojans and to create chipless RFID communications [1].

Previously, most EM side channel work was focused on lower MHz range frequencies, i.e., 1-10 MHz. Recently, GHz range frequencies have been investigated for EM [5], [8] and backscattering side channel analysis [1]. It is of interest to do this work with higher accuracy and in even higher frequency ranges and find ways to improve signal

quality at longer ranges. One possible way to achieve a higher quality signal at longer ranges is to use far field antennas. Far field antennas have been used to detect side channels at a distance. However, due to the inherently weak signal levels, antennas with more and more gain are needed to detect these side channels at distances exceeding a few meters.

In this thesis, a novel high gain planar quad antenna array with circular elements is designed. The design aims for a low cost and high scalability solution. To achieve this, each element is designed to operate at the higher $\boldsymbol{TM_{12}}$ mode, making each element larger and higher gain without introducing extra complexity to the feed network. Furthermore, the elements of the quad array are be fed by an electromagnetically coupled disc, further eliminating complexity in the form of transmission lines or dividers. The planar design of the ground and the elements are manufactured using inexpensive techniques such as waterjet cutting without using PCB manufacturing processes, which also would result in a far sturdier final product. The proposed antenna is then measured for return loss, gain, and pattern.

With the antenna manufactured and characterized, the proposed antenna is then used to measure the radiated emissions from the various embedded systems and Internet-of-Things (IoT) boards, at various distances under two conditions: direct Line of Sight (LoS) and Non-Line of Sight (NLoS). In addition to this, the SNR behavior of these side channel signals is evaluated with respect to distance. Due to the fact that these embedded systems create irrelevant radiation and noise of its own, calculation of SNR is more complicated than a simple thermal noise SNR characterization. This behavior is also analyzed and characterized.

1.3 Hardware Trojan Detection via Backscattering

It is possible to find ICs in practically every modern electronic device. Since they are so common, it is all the more important that these ICs are secure and authentic. In order to create ICs in the most efficient way possible, many different entities take part in the workflow. The more entities that take place in this process, the more opportunities there are for the IC to be maliciously tampered with. Malicious modifications that change the circuit or its hardware are called Hardware Trojans (HTs). The existence of HTs is very problematic in the context of software security because even the most secure software still has to rely on the hardware functioning as intend [9].

Because it is difficult to ensure the security of the manufacturing workflow, and because the risks created by compromised hardware is so significant, it is very desirable to have ways of detecting HTs in the final product. A promising non-destructive technique in HT detection is through side channel analysis [10], [11]. Since the technique relies on analog signals created unintentionally under normal operation, there is no modification required on the device under test.

Recently, the phenomenon of backscattering has been used to create a new type of EM side channel for detecting HTs in ICs [12]. This technique differs from regular EM side channels, which are created by current fluctuations in the IC due to the operation performed on the IC itself. Numerous applications including radars, RFIDs, etc. use EM backscattering. In many applications like radar, far field backscattering is used where the antennas are placed many wavelengths away from the observed object. Alternatively, near field backscattering is used in applications such as RFID technology [1]. Most existing

setups for this have the transmitting and receiving structures in different locations, which creates a problem in detecting HTs due to the fact that HTs are usually localized to a small region on the IC. In order to detect backscattering from only the relevant part of an IC, the setup needs to be able to focus in on regions that are 1 mm in diameter or smaller.

A straightforward way of achieving such a resolution in a backscattering sensing setup would be by using near field probes. In [12], it has been shown that HT detection is possible using near field probes in a backscattering setup. This fully off-chip setup was shown to be an effective dormant HT detection scheme. However, even though the near field backscattering setup was successful in detecting HTs, the electromagnetic mechanism behind the technique was not investigated in detail. Moreover, the measurement setup used commercially available E and H field probes, which are not necessarily optimal for the particular task due to their level of spatial resolution.

Microwave E field probes with high resolution that use open-ended coaxial cables are presented in [13], [14], and those that use printed circuits boards are presented in [15], [16]. For high resolution probes, there is a tradeoff between resolution and sensitivity. Since side channel signals are not created intentionally, the power levels are very low; which means very high spatial resolution probes are not suitable for the task. In addition, the backscattering setup for HT detection requires E and H field probes to be very close to one another, which means the two probes need to be designed together and have their unintentional interactions characterized.

In this thesis, a combination of an E and H field probes that can achieve ~1mm resolution in the presence of one another are designed for the purpose of optimal HT

detection through nearfield backscattering. These probes are first simulated and measured individually, then they are simulated and measured in the presence of one another. Relevant interactions between them that may improve or degrade performance are characterized. Finally, they are used to measure the backscattered signal from an FPGA running an Advanced Encryption Standard (AES) code with and without an injected dormant Hardware Trojan. The differences in these measured signals are be analyzed to see if detection of a dormant Hardware Trojan is possible through this method. This technique was able to detect all HT's with 100% accuracy for a sample size of 40, showing the power of this approach. Additionally, a proof of concept EM-circuit co-simulation is used to improve the theoretical understanding of this novel phenomenon of side channel emanation in the form of unintentional backscattering.

1.4 THz Near Field Focusing and THz Backscatter Side Channels

For the application of side channel detection, the THz band has great advantages over GHz band due to its wider bandwidth and less interference. The wide bandwidth (on the order of tens of GHz) available for backscattering side channel measurements in THz bands can provide tens of samples per nanosecond. This allows for the analysis of switching activity from one clock cycle to another along with the activity within each individual clock cycle. In addition, lower frequency bands have very strong outside sources of interference, such as cell phones, satellite radio, AC power, AM, FM, etc., and, most importantly, interference caused by other irrelevant components on the same circuit board or IC; whereas, this problem does not exist in THz bands [17]. Also, the smaller wavelength of THz bands allows for beams to be focused on small regions of an IC rather than the whole chip, which is very beneficial for side channel monitoring. For the applications of

HT detection and chipless RFID, this ability to focus on small regions can be very useful [1]. To be able to receive side channel signals related to these backscattering applications, near field focus antennas or highly directive antennas are required.

Many different structures have been used in the past for a near field focus. For example, at microwave frequencies, this has been done by approaches that include hybrid structures using substrate integrated waveguide SIW technology [18], Fresnel zone plate [19], [20]; microstrip [21], [22]; and reflect array antennas [23], [24]. At THz frequencies, near field focusing is achieved in [25], [26]. In the case of planar antennas, the size of patch elements creates fabrication difficulties, which require more expensive techniques to solve such as microfabrication, electron beam lithography. Newer fabrication techniques, such as 3D printing and electroless metal plating, can be used to manufacture a 3D printed Cassegrain reflector system that would be able achieve near field focusing at THz frequencies. This technique would allow for rapid prototyping and be less expensive [27]; moreover, it has not been used to create near field focused reflectors before.

There are many ways to design a near field focused reflector. Most straightforward technique is using reflector with an elliptical profile [28]. However, another method that is by axially displacing the feed in relation to the reflector system [29]. This method has the particular benefit of starting off as a far field design, which is useful for the cases of reconfiguring the antenna for different focus properties and switching between the far field and near field.

In this thesis, in order to have fast and inexpensive prototyping with better modification possibilities, 3D printing is used for reflector manufacturing as mentioned.

The nonidealities caused by 3D printing such as the conductive finish and surface roughness are be analyzed. The properties of the near field focus is to be measured and compared with the theoretical behavior.

With the THz reflector focuser manufactured and characterized, backscatter side channel measurements were conducted to demonstrate the performance of the proposed THz near field focuser. It was shown that the proposed near field focuser can effectively amplify the received backscatter signal and increase distance range, which is of critical importance due to THz (300 GHz) signal's high attenuation with distance. The backscatter side channel is created by switching activity of transistors in digital electronic circuits, such as microprocessors. This is tested using an implementation of a four-bit RFID design as described in [1] in Altera DE0-Cyclone V FPGA.

1.5 Polarization and Spatial Signal Variations of THz Backscattered Side Channels

Due to THz backscattered side channels being a very new area of research, there is no prior research regarding the polarization of these signals nor is there any analysis of the spatial variations of the backscattered side channel signals. To this end, we build further upon the work introduced in Section 1.4 previously.

Owing to the complex nature of connections on the FPGA board such as bondwires, circuit traces, high density of transistors, power connections, etc., there is limited knowledge and understanding about the spatial variations and the polarization of the backscatter signal that is modulated by the program activity of the FPGA. As compared to scattering from a uniform passive surface such as metal or insulator, the backscattered signal modulated by program activity shows significant variance based on the incident

signal location. Also, the behavior of the received power and SNR vs. distance is not known.

In this thesis, we explain and model the polarization effect using EM-circuit co-simulation. Equipped with the better understanding of the effect of polarization in THz backscattered side channels, the SNR enhancing effects of polarization on the received modulated backscatter were presented. Additionally, the spatial variations of the signal backscattered from the FPGA is studied. In particular, the ability to focus and isolate the signal from individual modules on an FPGA while limiting the interference from other modules is analyzed and it is found to be feasible. Lastly, we study and present the effect of distance of the receiver on SNR.

1.6 Thesis Outline

The rest of the thesis is organized as follows. Chapter 2 presents a brief background on far field antennas, near field focusers, and polarization. Chapter 3 presents the work towards improving side channel detection at a distance using far field antennas in the microwave band. Chapter 4 presents the work towards the design and analysis of a near field backscattering scheme for the detection of Hardware Trojans using side channels. Chapter 5 presents the 3D printed THz near field focuser that is then used for THz backscattered side channel detection. Chapter 6 presents the research regarding the effect of polarization in THz backscattered side channels. Finally, Chapter 7 concludes the thesis by summarizing the contributions and presenting possible future research directions.

CHAPTER 2. BACKGROUND

Design of electromagnetic sensors for different applications of electromagnetic side channel detection requires a detailed understanding of the concepts of far field antennas, near field focusers and polarization. In this chapter, we will provide a brief overview of the concepts related to far field antennas, near field focusers, and polarization that are frequently used in the rest of the thesis.

2.1 Far field Antennas

Far field antennas are structures that transmit or receive electromagnetic waves. They act as an interface between circuits and the medium where the electromagnetic waves travel large distances, typically distances much larger than both the wavelength of operating frequency and the size of the antenna itself. For our application, the ability to receive electromagnetic side channel signals at larger distances is as challenging as it is necessary, because these signals are inherently weak due to being created unintentionally and monitoring devices from the distance is often necessary. Deliberate design of an antenna is one way to enhance the range of such a system. This is a broad topic, so only a few of the concepts that are the most crucial in extending the range of EM side channel detection will be briefly covered.

2.1.1 An Isotropic Radiator

An isotropic radiator is a theoretical lossless antenna that radiates equally in all directions. In other words, an isotropic radiator that radiates power P_{rad} (W) will create an isotropic power density $W_0(r) = {}^{P_{rad}}/_{4\pi r^2}\ \left({}^{\mathrm{W}}/_{\mathrm{m}^2}\right)$ at a distance r (m), that does not

depend on direction of radiation. An isotropic radiator cannot be physically realized; however, it provides a very useful point of reference for quantifying how well an antenna performs.

2.1.2 Directivity, Efficiency, Gain, and Realized Gain

Antennas radiate more power in some directions than others, meaning the power density $W(r, \phi, \theta)$ for a real antenna will depend on the direction of radiation. The ratio of this power density to the isotropic power density W_0 for large distances, gives us the directivity D of the antenna. This ratio is usually expressed in dB scale. Unless a direction is specified, usually the highest value is reported.

Directivity quantifies how much of the radiated power is concentrated in a particular direction, however not all of the power sent to the antenna will be radiated. The factors that determine the ratio of the power radiated to the power sent to the antenna are called efficiencies, which are conduction efficiency e_c, dielectric efficiency e_d, and reflection (mismatch) efficiency $e_r = 1 - |\Gamma|^2$, where Γ is the voltage reflection coefficient. The total efficiency of the antenna is $e_0 = e_c e_d e_r$.

Gain and realized gain are terms that take efficiencies into consideration when quantifying the radiation properties. Gain is given by $G = e_c e_d D$, and realized gain is given by $G_{re} = e_c e_d e_r D$.

2.1.3 Friis Transmission Equation

Friis Transmission Equation, which can be used to determine the range of a radio link and the relationship between transmitted power and received power between two antennas is

$$\frac{P_r}{P_t} = e_t D_t e_r D_r \left(\frac{\lambda}{4\pi r}\right)^2 \tag{2.1}$$

where P_r is the power at the receiver, P_t is the transmitter power, e_t and e_r are the transmitter and receiver antenna efficiencies respectively, D_t and D_r are the transmitter and receiver directivities respectively, and r is the distance between the antennas.

2.2 Near Field Focusers

Unlike far field antennas which are intended to operate at distances much larger than the wavelength of the operation and the size of antenna itself, near field focusers are intended to operate at distances comparable to the wavelength of operation and the size of focuser itself.

There are different disciplines, such as microwave and optics, that work with near field focusers and there are different ways to define similar performance metrics. We have chosen a set of definitions discussed in the following text that were most suitable in the context of the application and allowed for an easy comparison with far field antenna definitions.

2.2.1 Near Field Focused Directivity and Gain

We use a near field focused directivity definition that is quite similar to the far field directivity definition. While the far field directivity is the ratio $W(r,\phi,\theta)/W_0(r)$ for large values of distance r, near field focused directivity is the same ratio for smaller values of distance r. Similarly, to find the near field focused gain and realized gain values, the directivity can be multiplied by $e_c e_d$ and $e_c e_d e_r$ respectively.

2.3 Polarization

Polarization is an important factor for electromagnetic waves, and it will be very relevant in Chapter 6. Electromagnetic waves are made up of coupled electric and magnetic fields and the behavior of the electric field determines the polarization. If the electric field is always along a particular direction, then the wave is said to be linearly polarized along that direction. If intentionally designed, this direction will be aligned horizontally or vertically to result in horizontal or vertical polarization which are orthogonal/perpendicular to one another. There are other types of polarizations, but they will not be particularly relevant in this thesis.

2.3.1 Role of Polarization in Direct Communication

Typically, the polarizations of the transmitter and the receiver are chosen to be the same. The results in maximum power transmission. In fact, if the transmitter and the receiver had exactly orthogonal/perpendicular polarizations, there would be no power transmission at all; which is a very undesirable situation. This is true for the simple case of transmitting a signal with a transmitter antenna and receiving it with a receiver antenna while hoping the signal is transformed as little as possible by whatever happens between transmission and reception.

2.3.2 Role of Polarization in Backscatter Communication

However, this is not the case for backscatter side-channel communications, which is what we work with in Chapter 4 and onwards. In that scenario, the transmitted signal is made to interact with an object, the signal is transformed by this objected, and that transformed signal is received by the receiver. *The transformation caused by this object is the only thing we are really interested in.* Specifically, in this thesis, the transformation we are interested in is in the form of a frequency shift that is caused by nonlinear and time-varying properties of the object. Additionally, since we are dealing with side channels, which are created unintentionally, the object is not designed interact with a specific type of polarization.

2.3.3 Polarization Filtering

As mentioned in the previous section, while detecting backscattered signals we are only interested in the part of the signal that is transformed by the object. Moreover, since we are specifically interested in unintentionally backscattered side channel signals in this thesis, the part of the signal that is transformed is much weaker than the signal that is not transformed – on the order of tens of thousands. Due to the way detectors work, the much stronger untransformed signal can *wash out* the desired part of the signal.

One important observation regarding this transformation is that it does not necessarily preserve the polarization. The transmitter can be vertically polarized, but the resulting backscattered signal can be mostly horizontally polarized, for example. This depends on the object under test. However, the untransformed part of the signal preserves

polarization. So, by filtering out the untransformed polarization, we can combat this washing out effect.

The concept of polarization filtering is commonly used in optics. One example makes use of the polarization transforming property of plastics. Depending on the stresses in a piece of plastic, the light is refracted differently. If optical polarizers are used to filter out the kind of polarization that is untransformed, colourful patterns can be seen as shown in Figure 1. These patterns exist in every transparent piece of plastic, except it is difficult to see because it is washed out by the untransformed polarization.

Figure 1 Plastic cutlery viewed in between two optical polarizers [30].

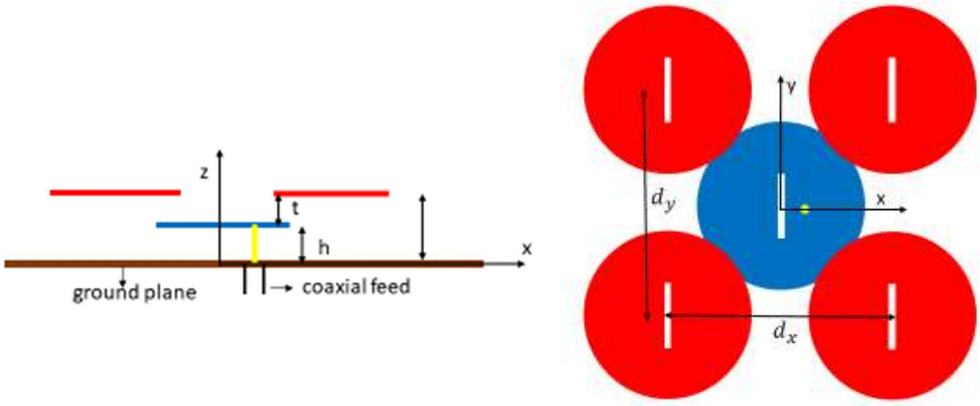
CHAPTER 3. A DIRECTIVE ANTENNA BASED ON CONDUCTING DISCS FOR DETECTING UNINTENTIONAL EM EMISSIONS AT LARGE DISTANCES

3.1 Overview

A novel high gain planar antenna is designed for long range EM side channel detection. Scalability was a key factor so that the detection range can be extended in a straightforward manner by increasing the number of elements cost effectively. The antenna consists of two layers of slotted conducting metal discs suspended on air and placed above the ground plane using teflon screws. The circular discs are designed to operate in the higher order TM_{12} mode, this allows for each element to have higher directivity with a simpler feed network. The screws' locations correspond to the electric field nulls along the disc radius. The upper layer is 2×2 array of slotted circular discs electromagnetically coupled by a lower identical disc which is fed directly by a single coaxial feed. The complete fabrication of the antenna is done using aluminum sheets and involves no of dielectric substrate. The antenna has a peak gain of 19 dBi with impedance bandwidth ($S_{11} \leq -6$ dB) of 6.7%. The antenna is tested for the application of receiving unintentional EM emanations generated by one or multiple embedded, "smart" electronic systems. Finally, the antenna was used to characterize the complex SNR behavior of EM emanation detection at a distance.

3.2 Antenna Geometry & Design

This section describes the proposed antenna geometry. The antenna is a two layer stacked configuration as shown in Figure 2 (a).



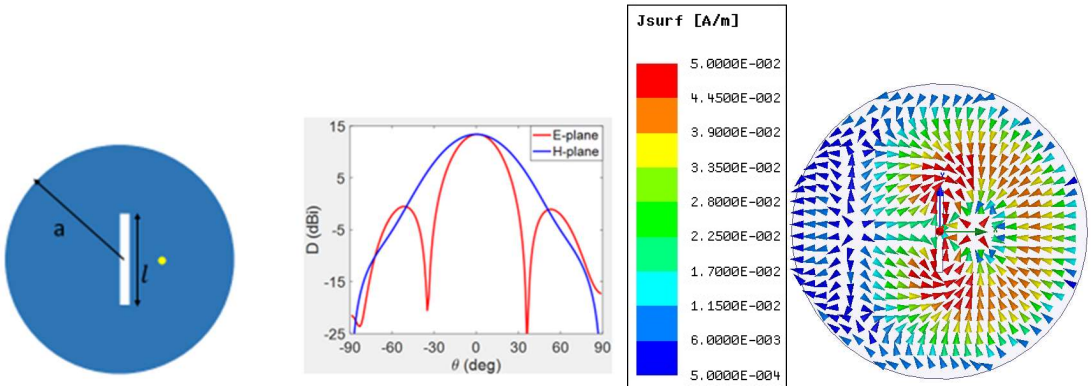
(a) (b)

Figure 2 Antenna Geometry (a) side view and (b) top view.

The upper layer is 2×2 array of slotted circular discs in TM_{12} mode, shown in Figure 2 (b), fed by an identical disc in the lower layer, which is directly fed by coaxial probe. A similar feeding technique was proposed in [31] where a 2×2 array of rectangular patches was excited by a microstrip fed and centrally located patch in the lower layer. This technique removes dependency on feed lines. Here, to avoid feed lines, we use coaxial feed to excite the lower disc. All circular discs have identical geometrical dimensions. The individual circular disc is loaded with narrow rectangular slot at the center. Slot loading is used to reduce the high sidelobes in the E-plane radiation pattern of TM_{12} mode, as explained and discussed in [32].

The design procedure is described as follows. Based on the peak directivity requirements, the single element is designed first as shown in Figure 3 (a). In the present case, the slot length is selected for maximum directivity, which is 13.4 dBi. The corresponding disc radius and slot length, *l,* are 20.5 and 11.3 cm respectively. Since it is a narrow slot, the slot width, *w,* is selected to be 1 cm. The thickness, *h,* is chosen to be 5 mm. Higher thickness values will result in increase in Side-Lobe Level (SLL) of the

element as explained in [32]. The directivity pattern of the single element in the E and H-plane and its current distribution is shown in the Figure 3 (b) and Figure 3 (c) respectively. The current density is higher in the region adjacent to slots compared to the other parts of the patch as the narrow slot at the center intercepts the flow lines of current and gets excited. This produces the out of phase electric field at the slot aperture, which leads to sidelobe cancellation as explained in detail in [32]. The 2×2 array of identical elements is then placed at the height t above this layer as shown in Figure 2 (a). In this case, the t is selected to be 5 mm. The array spacing d_x and d_y is chosen to reduce E and H-plane sidelobe and to improve impedance match ($S_{11} \leq -6$ dB). Additionally, the parameters of the center disc in the lower level can also be adjusted to improve the impedance match which also results in the reduced H-plane sidelobe (see more details in Section 3.3).



(a) (b) (c)

Figure 3 Element design at 1.03GHz: (a) Slot loaded disc, (b) directivity pattern in E and H-plane, (c) the current distribution of the patch.

3.3 Element Spacing, Side-Lobe & Impedance

In this section, we investigate the effect of array spacing and positioning of the center disc on the sidelobes in the radiation pattern. This is required since the element

radius is $\sim 0.7\lambda_0$ and hence the minimum array spacing will be greater than $1.4\lambda_0$. For the spacing greater than $1.4\lambda_0$, array theory predicts that the sidelobe will be high in the radiation pattern, which reduces the aperture efficiency and the directivity [33]. In antenna arrays, several methods have been used in the past for sidelobe suppression [34], [35]. In this design, the side lobe in the E-plane is suppressed by the slot loaded in the disc. In the H-plane the sidelobe is suppressed by the center disc. This is explained in Section 3.3.1. In addition to that, in Section 3.3.2, we show the effect of lower disc parameters like slot length and disc radius on the impedance match of the antenna. The radiation patterns at the various frequencies in the band are also discussed in this section.

3.3.1 Element Spacing & Side-Lobe

To explain how element spacing impacts the sidelobe, we investigate E & H-plane radiation pattern of 2×1 array and 2×2 array of the element shown in Figure 3 (a), assuming infinite ground plane configuration. Figure 4 (a) & (b) shows the geometry of 2×1 and 1X2 array. Simulations were performed for the various spacing between array elements for both the geometries. Current distribution for both array geometries are shown in Figure 4 (c) & (d). For both elements, the excitation amplitudes are equal with zero phase difference. Current density scaling is the same as used in Figure 3 (c). It is observed that 2X1 array compared to 1X2 array has strong current density around the slot edges. The reason for this is the aperture field vector of the slot, which is in the direction of x-axis, as explained in [14], and hence can have possible coupling effects in the 2X1 configuration.

Figure 5 (a) & (b) shows the E & H-plane pattern for 2X1 array geometry with element spacing d_x as parameter. As d_x increases from 1.5 to $2\lambda_0$, the first sidelobe in the

E-plane increases. For $1.5\lambda_0$, there is one lobe in the visible region while for 1.75 and $2\lambda_0$, there are two lobes. In all cases the minor lobes are 10 dB below the main beam. Figure 5 (b) shows that element spacing has negligible effect on the H-plane pattern.

Figure 5 (c) & (d) shows the E & H-plane pattern for 1X2 array geometry shown in Figure 4 (b). Compared to Figure 5 (a), H-plane pattern shown in Figure 5 (d), has higher sidelobes since the sidelobe cancellation effect of slot is less dominant in the H-plane configuration. The first sidelobe is reduced by ~ 3dB in the E-plane of 2X1 array, due to cancellation effect by slot loading, as compared to the H-plane pattern of the 1X2 array. Based on this study of how the array spacing impacts radiation pattern, we chose the value of $1.75\lambda_0$. We have also observed in simulations that the selected spacing has a good impedance match in the frequency band of interest. This is also shown in Figure 7 (a).

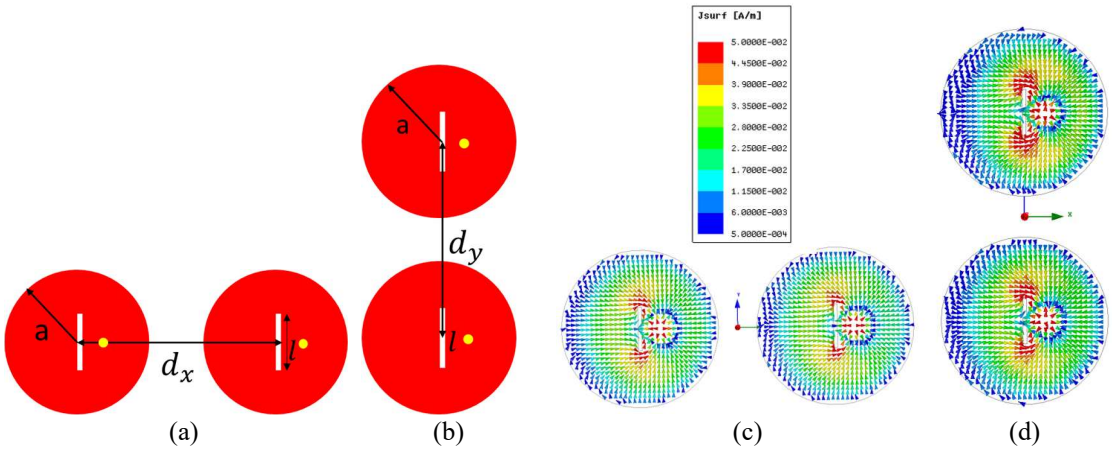


Figure 4 Array geometry (a) 2X1 array (b) 1X2 array (c) current distribution of 2X1 array, (d) 1X2 array.

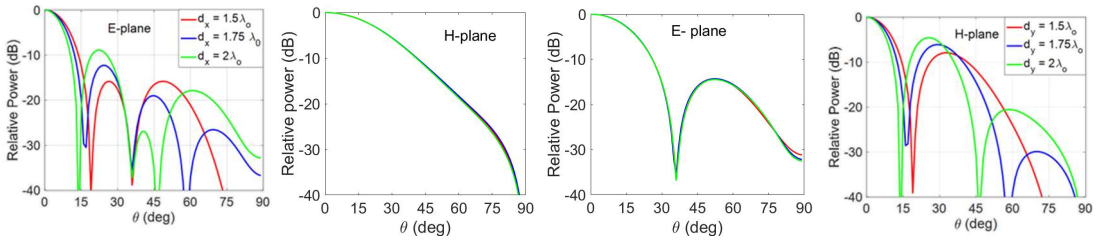


Figure 5 Radiation pattern as a function of array spacing (a) & (b) E & H-plane pattern for geometry shown in Figure 4 (a), (c) & (d) for the geometry shown in Figure 4(b).

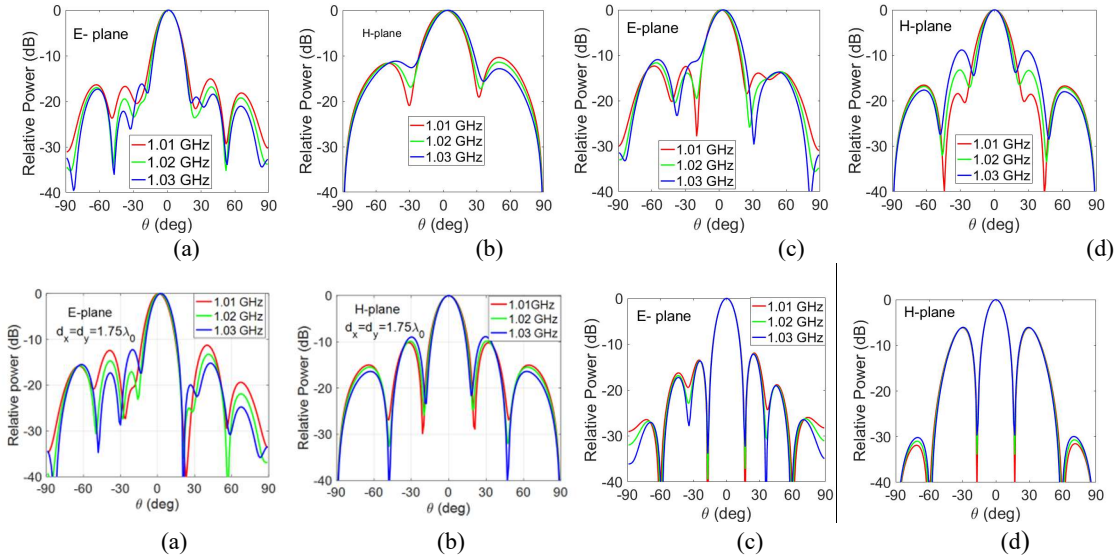


Figure 6 Effect of the center disc on the radiation pattern in (a) 2X1 array E-plane, (b) 2X1 H-plane, (c) 1X2 E-plane, (d) 1X2 H-plane, (e) 2X2 E-plane, (f) 2X2 H-plane, (g) 2X2 array without lower center disc, E-plane, (h) 2X2 array without lower center disc, H-plane.

To excite the array, an identical disc is placed at the center of the ground plane, at smaller height than the upper four discs as shown in Figure 2 (a). Figure 6 shows the effect of the lower layer center disc on the radiation pattern of the antenna. Effect of the center disc on the radiation pattern was studied in 2X1, 1X2 and 2X2 array configuration, for the selected element spacing of $1.75\lambda_0$. Figure 6 (a) & (b) show the effect in the 2X1 array geometry. Compared to Figure 5, the sidelobes in the E-plane are reduced. In the H-plane,

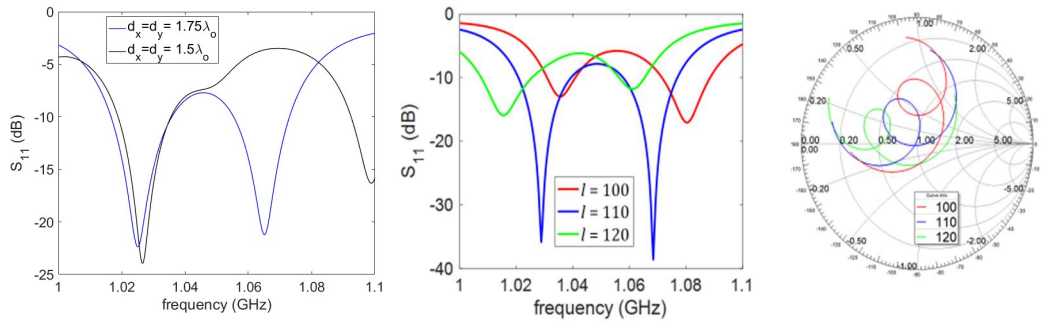
additional lobe is there in the visible region. Figure 6 (c) & (d) shows the radiation pattern when the 1X2 array geometry is loaded with center disc. Compared to Figure 5 (c) & (d), it is observed that sidelobes are suppressed in the H-plane and in the E-plane additional lobes are introduced with the distorted pattern. Figure 6 (e) & (f) show the radiation pattern of 2X2 array, with center disc loading. For the comparison, the radiation pattern of unloaded 2X2 array is shown in Figure 6 (g) & (h). Compared to the 2×2 array without center disc, the presence of the center disc reduces the sidelobe in the H-plane by ~ 3 dB. In the E-plane, the pattern peak is off the boresight by 2°, but the sidelobes are still ~ 10 dB below the main lobe.

3.3.2 Impedance Match

To make the design practical, the simulations are performed with finite ground plane. We choose 1.04 m×1.04 m squared ground plane made of aluminum, which resembles the fabricated antenna in the next section. It was shown in [31] that stacked configuration has wideband characteristics and the impedance match depends on the overlapping area of the two layers. In the present design, the additional parameter that can affect the impedance is the lower disc slot length *l*. Figure 7 shows the effect of the array spacing and the lower disc slot length on the S_{11} and the impedance over the frequency band. Each case displays two coupled resonances which corresponds to the upper and the lower layer. Figure 7 (a) shows that for the array spacing of $1.75\lambda_0$, the impedance match is obtained in the desired band. For closer spacing of $1.5\lambda_0$, due to resonance split around 1.045 GHz, there is a mismatch in the band. Hence the array spacing of $1.75\lambda_0$was selected for the design. Once the upper 2×2 layer geometry is fixed, the amount of coupling depends

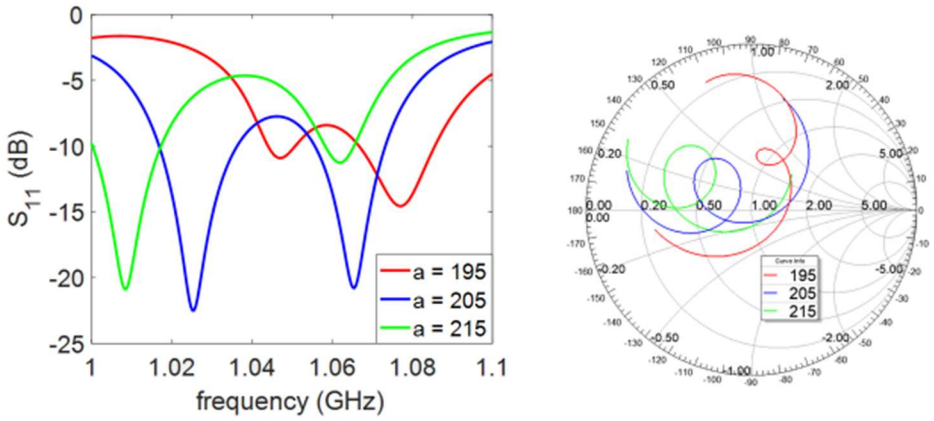
on the lower disc slot length. For l = 100 mm, the impedance is inductive as shown in the Smith chart in Figure 7 (c). Increasing slot length to 110 mm results in impedance match for the whole band, shown in Figure 7 (b). Further increase to 120 mm reduces the input resistance which results in impedance mismatch.

Figure 8 (a) shows the reflection coefficient vs. frequency with lower disc radius, *a,* as parameter. With an increase in radius, the resonances shift to lower values. Furthermore, Figure 8 (b) shows less coupling between two resonances due to smaller loop sizes in the smith chart, which increases with the disc radius. When the disc radius is 205 mm, the impedance is matched for the band. Slot length, *l,* for this case is 113 mm, which is also the selected length for the fabrication.



(a) (b) (c)

Figure 7 (a) Reflection coefficient vs frequency with array spacing as parameters (b) Reflection coefficient vs. frequency and (c) Impedance loci variation with lower slot length as parameter.



(a) (b)

Figure 8 (a) Reflection coefficient vs. frequency and (b) Impedance loci variation with lower disc radius a as parameter.

The simulated radiation patterns in the E & H-plane for four frequencies in the band of interest are shown in Figure 9 (a) and (b). The peak gain is above 18 dBi in the whole frequency band with a maximum value of 19.1 dBi at 1.03 GHz. The maximum cross polarization level in H-plane is ~ 20 dB below the main lobe in the entire frequency band. We observe in the simulations that with the increase in frequency, the H-plane sidelobe increases from -10.2 dB at 1.01 GHz to -7.7 dB at 1.04 GHz. This is because at the higher frequencies of the band the array spacing becomes larger and hence results in increased SLL. In the E-plane, the beam is shifted 2° from the maximum at 1.03 GHz.

The antenna geometry shown in the Figure 2 was designed, fabricated and tested. The center frequency of the designed antenna is 1.03 GHz. A square aluminum sheet of dimension 1.04 m was used as a ground plane. The individual discs have the radius of 20.5 cm with the slot length and width of 11.3 cm and 1 cm respectively. Each of them is fabricated using aluminum sheet of thickness 2 mm. The center disc is suspended at 5 mm above the ground plane while the other four are at 10 mm above the ground plane. The

center disc is directly fed by a 50 Ohm coaxial probe, which is placed at 50 mm away from the center. The fabricated antenna picture is shown in Figure 10.

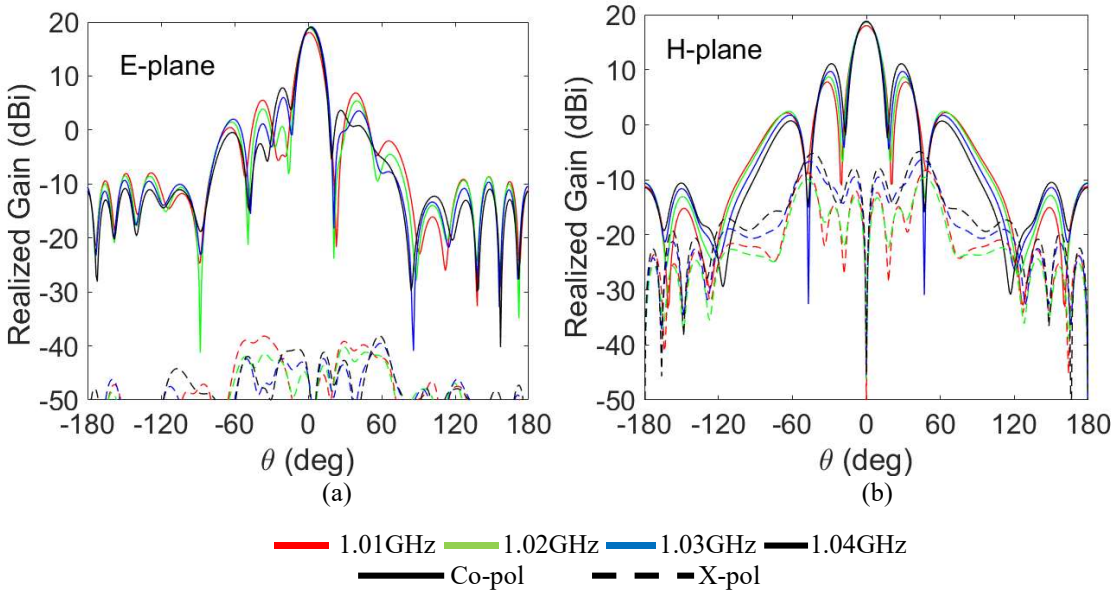


Figure 9 Radiation pattern over the band for the antenna geometry shown in Fig. 1 at (a) E-plane, (b) H-plane.

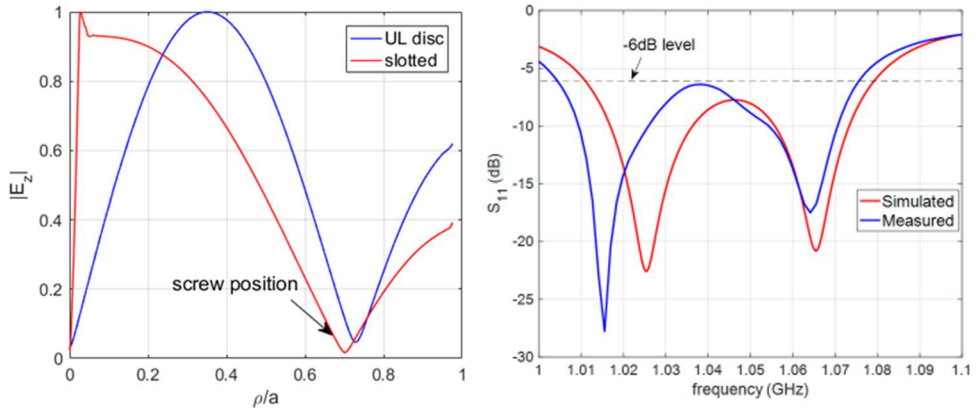
3.4 Antenna Fabrication & measurements

(a) (b)

Figure 10 Fabricated antenna (a) front view (b) side view.

Each disc is suspended using four Teflon screws. Modal electric field distribution of the TM_{12} mode is used to determine the position of screws. To explain this, Figure 11 shows the simulated electric field $|E_z|$ inside the cavity vs. normalized radius, for a single

unloaded and slot loaded disc. The $|E_z|$ of unloaded (UL) disc follows the first order Bessel function $J_1(k\rho)$ [10]. For UL case, the electric field null is at ~ 0.7a. We have observed that slot loading does not have significant effect on the position of electric field null as shown in Figure 11 (a). Compared to the fundamental mode, this property is an added advantage of TM_{12} mode since nulls in electric field allow us to suspend the patch on the air and hence eliminate the need for the substrate.



(a) (b)

Figure 11 (a) Simulated cavity electric field vs normalized radius (ρ/a) for unloaded and slotted disc operating in TM12 mode. (b) Comparison of simulated and measured S11 as a function of frequency.

Figure 11 (b) shows the simulated and measured reflection coefficient for the antenna shown. The difference between the measured and the simulated resonant frequencies is less than 1%. The measured $S_{11} \leq -6$ dB bandwidth is 6.7% or 70 MHz. It covers the required bandwidth for the side channel EM detection (shown later in section 3.5). Figure 12 (a) & (b) shows the mounted antenna picture and the measurement set up to measure the near field and far field patterns of the proposed antenna. The proposed antenna is used as a receiving antenna while the transmitting antenna is a standard broadband double ridge waveguide horn shown in the Figure 12 (b). A digital protractor

was used to measure the angle of rotation. The antenna patterns both near field and far field were measured at the roof top of Tech Square Research Building at Georgia Institute of Technology. The measurements were done for 3m, 5m (near field) and 15 m (far field) distance. The antennas were mounted at the height of 3.5 m above the ground. In the far field measurements, to reduce the specular ground reflections from the transmitting horn, the absorbers were used in the middle region of the measurement set up.

(a) (b)

Figure 12 Pictures of antenna measurements (a) mounted antenna (b) measurement setup.

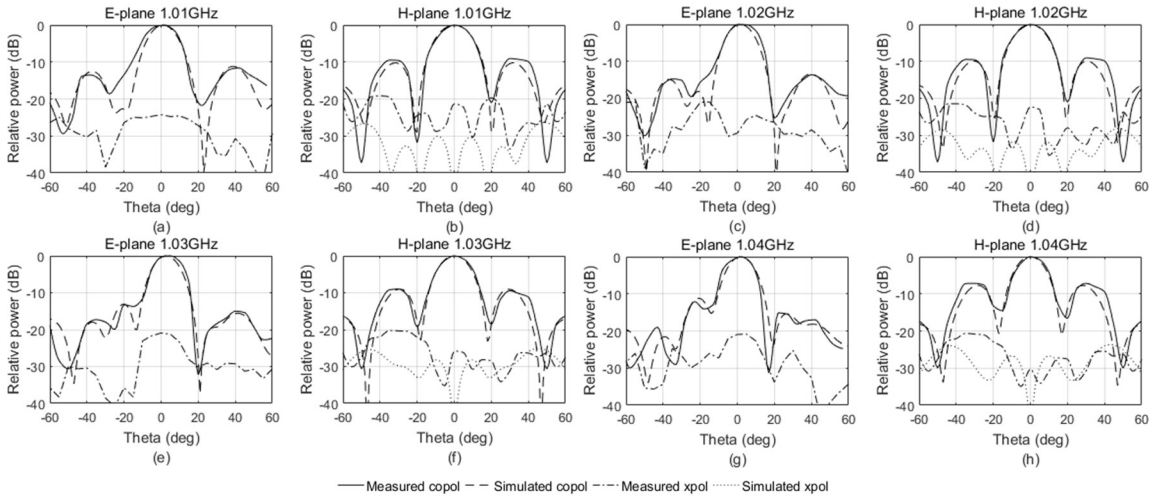


Figure 13 Simulated and measured radiation patterns in E and H-plane (a) & (b) 1.01GHz, (c) & (d) 1.02GHz, (e) & (f) 1.03GHz, (g) & (h) 1.04GHz (i) Comparison of simulated and measured realized gain as a function of frequency.

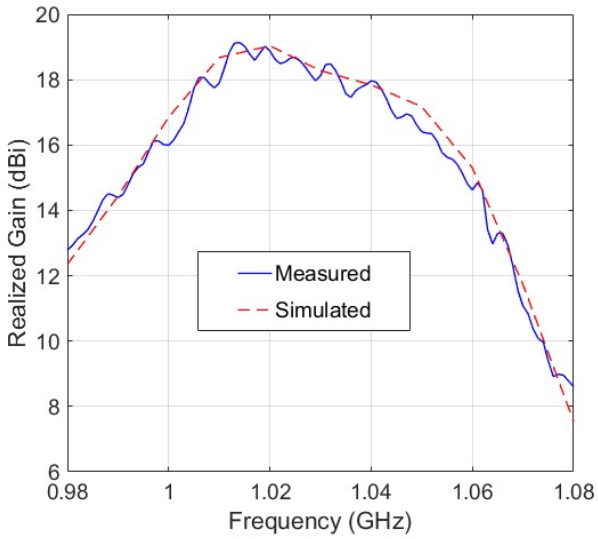


Figure 14 Comparison of simulated and measured realized gain as a function of frequency.

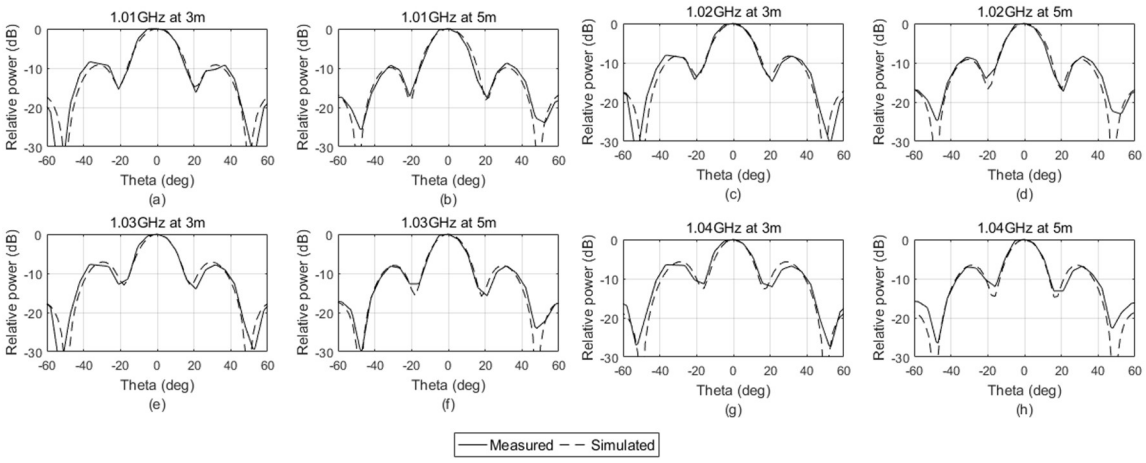


Figure 15 Near field relative power patterns at 3m and 5m distances from the antenna aperture, (a) & (b) 1.01GHz, (c) & (d) 1.02GHz, (e) & (f) 1.03GHz, (g) & (h) 1.04GHz

Figure 13 (a) - (h) shows the measured E & H-plane radiation patterns of the antenna, for the various frequencies in the band. The measured radiation patterns match well with the simulated ones. In the measured E-plane pattern at 1.03 GHz, the beam is shifted by 3° as compared to 2° in the simulations, also observed earlier in Figure 9. The measured cross-polarization is less than -21 dB and -19 dB, for the entire band in the E and

H-plane respectively. In Fig. 13, the simulated cross-polarization in the E-plane are less than -40dB also shown in Figure 9. Figure 14 shows the simulated and measured realized gain as a function of frequency for the fabricated antenna. For planar directive antennas, the peak gain and gain pattern measurements are conveniently conducted in the antenna measurement ranges. However, since we do not have access to antenna measurement ranges, we have verified the peak gain of the antenna by using the conventional gain transfer method [36], using standard horn. The measured gain matches well with the simulated one. Peak measured value is 19.2 dBi as compared to 19.1dBi in the simulations. The measured value is higher due to the ripples in the gain measurements, which are ~ 1.2 dB and are caused by the standing wave patterns in front of the aperture due to reflections.

Figure 15 shows the near field patterns of the antenna at 3 and 5m distances from the antenna aperture. Both the distances are in the radiating near field region of the antenna. The measured power pattern matches well with the simulated patterns. The measured maximum sidelobe level at 3 and 5m are -6.1dB and -6.6 dB respectively. It is observed that between 1.01 to 1.04 GHz, the maximum sidelobe level changes by ~ 3 dB, for both 3m and 5m distances. The antenna is used to receive the fields from the board processor at those distances as presented in the next section.

3.5 SNR Measurements & Malware Detection

The proposed antenna was used to measure the radiated emissions from the various embedded systems and Internet-of-Things (IoT) boards, at various distances under two conditions: direct Line of Sight (LoS) and Non-Line of Sight. These IoT boards typically consist of an ARM processor, a Flash memory, and a set of peripherals (e.g. WiFi modules,

etc.). IoT boards are typically used for controlling a variety of tasks in factory lines, hospitals, critical infrastructures, etc. Recently, there have been a growing interest in attacking these devices since both the number and importance of them are growing rapidly. Monitoring these devices using the EM side channel signals generated by them is one of the ways to improve the security of IoTs against cyber-attacks. Collecting stronger EM signals will improve the accuracy of the malware detector and that is the main goal of designing our proposed antenna.

3.5.1 Line of Sight (LoS) Measurements

Here, we will first describe the direct LoS measurements for the IoT board shown in Figure 16 in detail. Figure 16 (a) shows a diagram of the measurement setup and Figure 16 (b) shows the photo of the measurement setup where the proposed antenna is measuring the EM signal from an IoT device named Olimex [37] which has an ARM processor and runs a Linux operating system. The signal power measurements, using a spectrum analyzer (Agilent N9020A), were conducted at various distances between 1-5 m from the device. For each distance, two measurements were collected and the corresponding Signal to Noise Ratio (SNR) was calculated. Since it is not straightforward to estimate SNR for emanations from the electronic devices, we have conducted additional experiments to estimate SNR as described below.

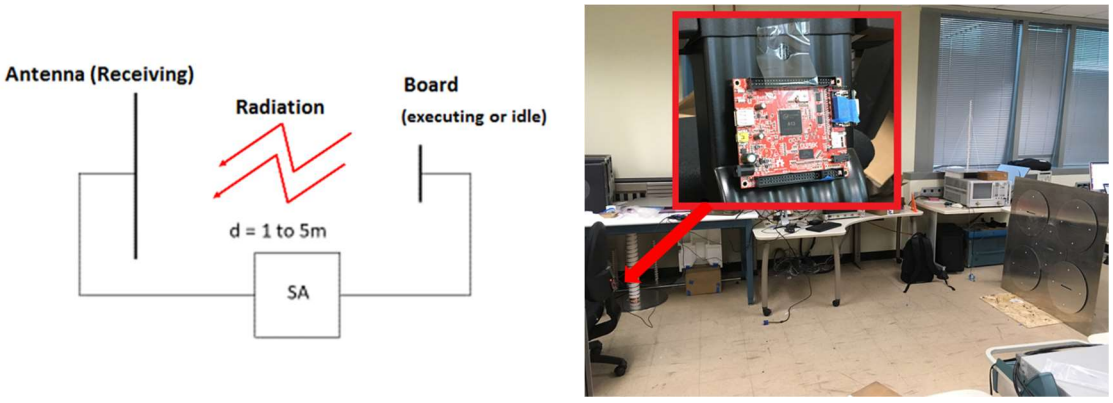
In the first set of measurements the objective is to estimate total emanated power, S, received when the board is on and running the program activity of interest. In the second set of measurements, the objective is to estimate the noise spectral power, N, received when the board is on but there is no application running (idle mode). The noise power here

includes thermal (N_{therm}) noise as well as emanations coming from the board itself (N_{board}) that are not related to the program activity. SNR is then calculated as:

$$SNR\ (dB)\ =\ S\ (dB)\ -\ N\ (dB) \tag{3.1}$$

$$\text{SNR} = \frac{P_{r_{executing}}}{P_{r_{idle}} + N_{thermal}} \tag{3.2}$$

where, $P_{r_{executing}} \propto \frac{P_t}{r^2}$ is the power received when the processor is executing the code, while P_t is the power at the input. $P_{r_{idle}}$ is the power received when the processor is turned on but not executing a code. This part carries no useful information, and acts as a source of noise. N_{therm} is the thermal noise, independent of distance.



(a) (b)

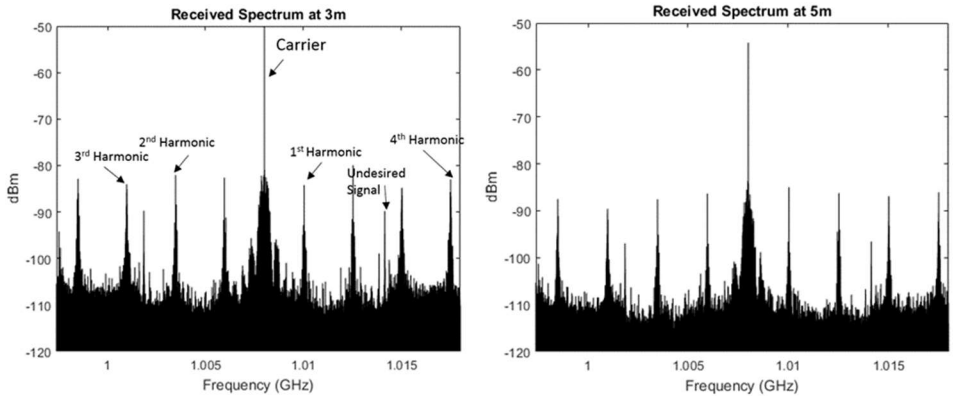
Figure 16 SNR Measurements for an IoT (Olimex) board: (a) Block diagram of set up (b) Set up picture that shows the antenna (on the right side) and the board (on the left side).

The proposed antenna is used to receive electromagnetic radiation coming from the board's processor. The objective is to find the possible malicious activities by analyzing the program execution through EM emanations. The main idea behind the malware detection method is that since there is a correlation between the program activities and the

generated EM signals, executing a certain application will generate unique and distinguishable signatures in the EM signal. Thus, by collecting these EM signals for each application and extracting the signatures, a reference model for each application can be built. Then during monitoring, if an attacker changes the application's code, this will result in generating different EM signals that no longer match with the model and hence can be detected. Further details can be found in [5], [8].

The signature extraction is based on the premise that a program spends most of its time executing some repetitive code (e.g. loops) which results in prominent peaks appearing in the spectrum separated by $\Delta f = {}^{1}/_{T}$, where T is the duration of a single loop iteration. In addition of base-band signal where these loops can be observed, they can also be observed as a modulated signal around the processor clock frequency (in our case 1 GHz), which is the signal we are observing. Measured power spectrum at the distances of 3 m and 5 m are shown in Figure 17 (a) and (b) respectively. From Figure 17 (a), we can observe that the strong spectral lines are amplitude modulated by a clock frequency (which acts as a carrier) of 1.008 GHz, which is significantly stronger than everything else. Each of the labeled harmonics are approximately 1.95 MHz apart from one another, which indicates that each iteration of the loop in the code takes about 514 ns. Since the board has many activities going on at once, it creates some other signals that are not related to the code that is being run on the processor. An example of this is marked as undesired signal in Figure 17 (a).

Figure 18 (a) shows the measured SNR for various distances in comparison with the SNR obtained by a theoretical model defined in (3.2). The theoretical fit agrees well with the measured SNR.



(a) (b)

Figure 17 Measured signal power while code is executing at various distances (a) 3 m and (b) 5 m.

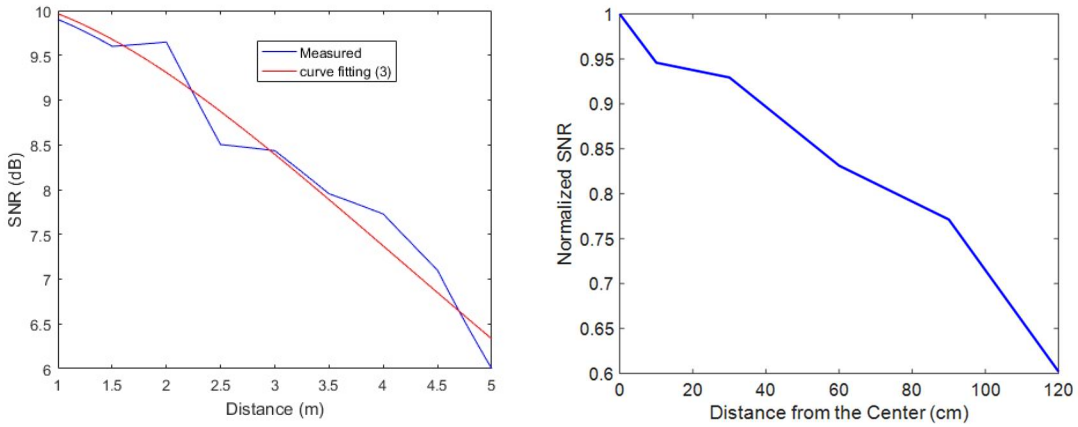
To explain the measured SNR, with the theoretical model, the noise observed in the measurements is assumed to be created by two sources: thermal noise and the noise generated by the board itself. Since the processor is not intended to function as a transmitter, only a part of the total radiation coming out of the board carries meaningful information. This undesired part of the radiation lowers the quality of the signal. Since this part of the signal is radiated from the board, it gets weaker by a factor of r^2 , whereas the thermal noise is constant, as pointed out in (2). For this reason; at smaller distances $P_{r_{idle}}$ is more significant, at larger distances N_{therm} is more significant, and at intermediate distances the SNR trend is neither constant nor r^2.

SNR fit is given as:

$$SNR_{fit} = \frac{\frac{a}{r^2}}{\frac{b}{r^2}+c} \tag{3.3}$$

$$SNR_{fit}^{-1} = \frac{b}{a} + \frac{c}{a}r^2 \tag{3.4}$$

It can be seen that SNR_{fit}^{-1} is a linear function of r^2 and the data points were fitted using linear least squares method. The multiplicative inverse was taken of the resulting line, which fitted the data very well.



(a) (b)

Figure 18 (a) Measured SNR vs. distance in comparison with the theoretical model fit. (b) Measured normalized SNR vs offset distance from the LoS (SNR = 1 corresponds to LoS).

3.5.2 Non-LoS Measurements

As mentioned earlier, the proposed antenna is designed so that it can be hanged on the wall and received the EM signals from electronic devices that are active in a room. In this scenario, not all the monitored devices would be in the LoS but the antenna should still be able to monitor them. In order to use the EM signals for malware detection, the spectral peaks (as shown in Figure 17) should at least be 1 dB higher than the noise floor. In other

words, in order to be able to monitor non-LoS devices, the receiving signal should have peaks with at least 1dB higher than the noise floor.

To evaluate the effectiveness of our design, we repeat the measurement in Figure 16, this time with moving the board toward up-down and/or left-right directions from the center of the antenna with the step of 10 cm. All measurements are done while the center of the board is 3 m away from the center of the antenna. For each step (i.e. different distances from the center of antenna while being 3m away from it), we measure the SNR for the receiving EM signal. Figure 18 (b) shows the results for the weakest peak in the test application.

As shown in the Figure 18 (b), the antenna can receive EM signals with only 30% decrease in SNR while being 1 m away from the center of the antenna. However, our measurements show that beyond 1m, the SNR decreases dramatically. This is due to directive beam in both E and H-plane.

3.5.3 Malware Detection

Finally, to illustrate how well the proposed antenna works in the system for malware detection, we use the antenna to receive EM signals while we are running several standard embedded systems applications such SHA, Djikstra's path-finding algorithm, QSort, CRC32, and FFT from a standard benchmark called *MiBench.* We also implement two real attacks: one a Distributed Denial-of-Service (DDoS) attack, and the other a Ransomware attack. We run the applications first 25 times without having any attack on them (benign), and 25 times with the DDoS attack, and 25 times with the Ransomware attack. We then used an algorithm proposed in [5]to analyze the receiving EM signals and

label each run as either “benign” or “malicious”. We then calculate False Positive Rate as the number of runs that were incorrectly labeled as “malicious” divided by the total number of runs. Similarly, True Positive is defined as the number of runs that are correctly labeled as “malicious”.

Our results show that for all the applications while measuring from 3m, 4m, and 5m distances, we can perfectly find all the instances of the malware while achieving 0% false positive rate which confirms that our designed antenna is suitable for receiving EM signals from such devices from >3 m distance. Note that the results in [5] were reported while measuring from 5cm distance from the board and collected by a probe.

3.6 Conclusions

In this research, a high gain planar slotted circular disc antenna, designed for receiving EM emanations modulated around processor clock was presented. The antenna was designed around 1 GHz for a 70 MHz bandwidth, using higher order mode TM_{12} mode, which had a larger electrical size than the fundamental mode. This was done to reduce the number of elements. The antenna was designed in stacked configuration which permits the use of EM coupling as an excitation and hence feed lines were avoided. The antenna was fabricated using aluminum circular slotted discs, which are suspended in air using Teflon screws. It was shown that the electric field null property of TM_{12} mode allows the use of screws to suspend the discs above the ground plane. The signal detection at the distances greater than 3 m were demonstrated by direct LoS SNR measurements from an IoT board. For each distance, SNR was calculated by subtracting the detectable signal power, when board activity is on, with the noise power when there is no activity. Finally, the antenna

was used to collect EM signals from an IoT board while being >3m away from the board. The results show that using this antenna, an IoT board can be monitored from >3 m with excellent accuracy. Furthermore, the antenna is cost effective and can be treated as a sub array for larger array for going further distances in EM emanations measurements.

CHAPTER 4. NEAR FIELD BACKSCATTERING FOR HARDWARE TROJAN DETECTION

4.1 Overview

This study presents the near field measurement setup and the sensor topology used to measure the backscattered signal from a small spot of ~1 mm on an FPGA to enable Hardware Trojan (HT) detection. A novel sensor topology used in the setup contains a combination of E and H field probes, which is used to excite a carrier and receive the modulated scattered signal that carries a signature of the inspected logic circuit. As a proof of concept and to develop insight, an EM-circuit co-simulation is presented to show that received signal contains a signature of the logic circuit under test imprinted on the relative power levels of the modulated scattered clock harmonics. The received modulated scattering signature was successfully used to detect the presence of a HT in the original circuit. In the sensor topology; the effects of using E and H field probes in very close proximity, such as resolution and mutual coupling, are analyzed and discussed. Also, it is shown that there is negligible effect on the spatial resolution and the invasiveness. The probe combination is shown to have a spot size of ~1 mm, and a coupling isolation better than 20 dB in the frequency band of interest.

4.2 Hardware Trojans & FPGA

This section describes the particular HT selected in this study and the particular FPGA it was implemented on along with the physical sizes associated with the HT and the rest of the logic circuit which implements Advanced Encryption System (AES).

To be able to quickly switch between HT-injected and HT-free circuits, an FPGA is used. The specific FPGA board that is used is the Altera DE0 board with a Cyclone V FPGA. Using an FPGA to test both HT-injected and HT-free logic circuits make it possible to eliminate all other variations apart from the difference the HT itself makes. In order to understand the impact a HT has on EM emanations, it is important to understand the different components of a HT and how they function.

A HT ordinarily contains two parts: the trigger and the payload. The trigger will not activate the payload unless very specific conditions have been met, and these conditions are usually designed such that it will not be activated during testing. These dormant HTs are much more difficult to detect compared to activated HTs; however, since they are most likely to remain dormant during testing, it is important that the testing method can detect HTs while they are dormant. Furthermore, these HTs can be modified to have smaller size to make detection even more difficult.

Backscattered side channel measurement set up used to detect HTs in [12] involves commercial probes. Aaronia E1 electric field and H2 magnetic field probes were used. The device under test was FPGA chip on Altera DE0-CV board and is positioned beneath the probes. The backscattered signal was received by H2 probe which has a diameter of 2 cm. It was found that the detection accuracy of HT's decreases as trigger's size reduces to ¼ of the original size of the trigger. In other words, the near field backscattering technique depends upon the size and the location of the HT trigger and hence for a HT detection of smaller sizes, it is desirable to have transmitted and received probes that have higher spatial resolution.

To develop intuition about the physical size of the smaller HT's trigger, in this paper, we are using an AES circuit with a HT. This Trojan is suitable for investigating the effects of size and localization [12]. The particular HT that is used in this study is the AES-T1800 HT benchmark found on TrustHub [38]. This HT includes a trigger that uses combinational logic and waits for a specific 128-but AES input. Once activated, its payload cyclic shift register activates and continuously operates to increase power consumption. This can be very disruptive for small electronics that depend on low power consumption and energy harvesting such as medical implants. The diagram of an AES circuit with and without the HT is shown in Figure 19. The scale of the original logic circuit on the FPGA and the size of the HT can be seen here.

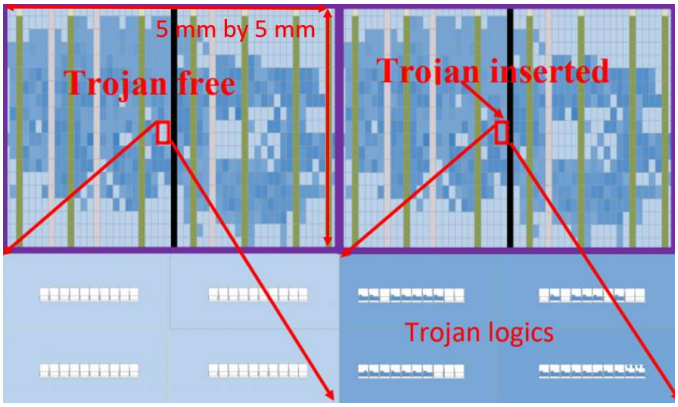


Figure 19 The FPGA logic layout for the Trojan free and Trojan inserted cases. Size of the FPGA is 5 mm by 5 mm.

4.3 Near Field EM Sensor

This section presents the E and H field probe combination that is used as a near field EM sensor to detect modulated scattered signals from a small localized region on a ICs or FPGAs. Design and fabrication of this sensor topology is explained in subsection A

while the spatial resolution, coupling isolation, and invasiveness are discussed in subsection B.

4.3.1 Design & Fabrication

We use an electric monopole above the ground plane and the short helix wound at its tip to detect the scattered field from a ~1 mm size the region of the FPGA. A multi-turn loop probe in the vicinity of the monopole will have less mutual coupling owing to the orthogonal nature of the fields. Figure 20 show the geometry of the combination. The E field probe is used as a transmitting probe for incident power and H-field probe is used as a receiving probe to receive unintentionally modulated and scattered signals from an FPGA.

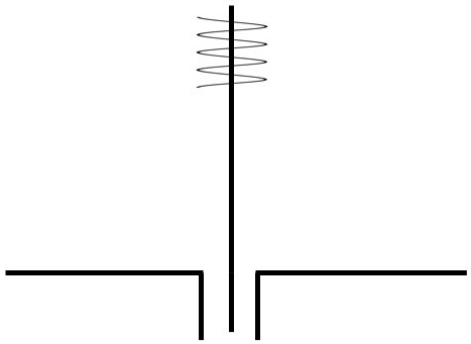


Figure 20 monopole and multi-turn loop combination.

Figure 21 shows the geometry of the proposed E and H field probes. The variable d is used to describe the vertical distance between the tip of the E field probe and the device under test. In this study we use the values 0.2 mm and 0.5 mm for d. The dimensions of the sensor geometry are shown in Table .

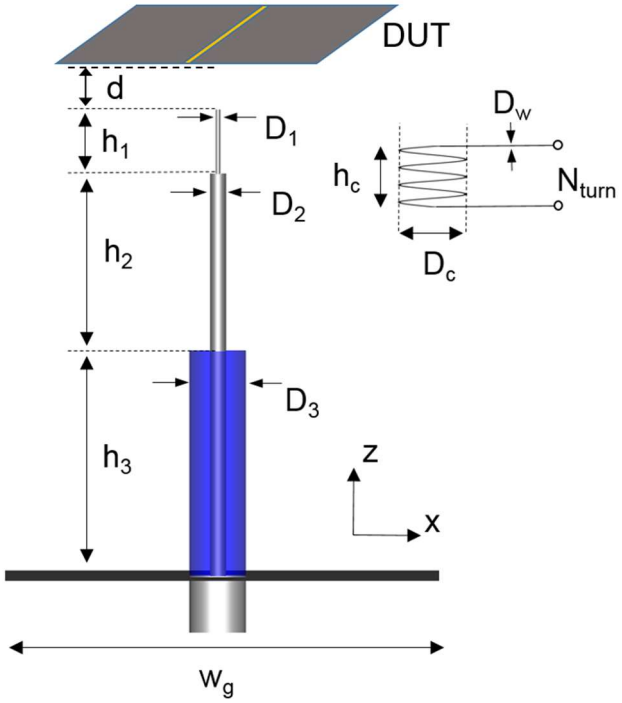


Figure 21 E field probe geometry and design.

Table 1 Design parameters (in mm) for the monopole probe shown in Figure 21.

$\boldsymbol{D_1}$	0.2	Diameter of the tip of the conductor
$\boldsymbol{D_2}$	1.27	Diameter of the base of the conductor
$\boldsymbol{D_3}$	4.1	Diameter of the extended PTFE sleeve
$\boldsymbol{h_1}$	4	Height of the tip of the conductor
$\boldsymbol{h_2}$	25	Height of the base of the conductor
$\boldsymbol{h_3}$	15	Height of the extended PTFE sleeve
$\boldsymbol{w_g}$	34	Edge length of the square ground plane
$\boldsymbol{D_c}$	2.5	Diameter of the H probe coil. Wound around PTFE
$\boldsymbol{D_w}$	0.35	Diameter of the H probe coil wire.
$\boldsymbol{h_c}$	2.2	Height of the H probe coil
$\boldsymbol{N_{turn}}$	6	Number of turns for the H probe coil. Wound tightly.

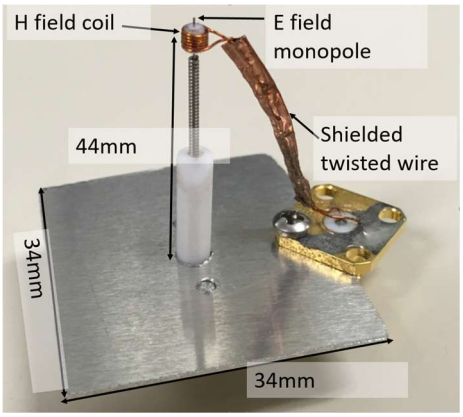


Figure 22 Fabricated sensor prototype.

Since certain modules in an FPGA would be localized, it is beneficial to have fine spatial resolution. However, there is a tradeoff between the fine spatial resolution and the sensitivity. Since the mechanism of backscatter is unintentional, the signals we are trying to detect are inherently week. Too fine of a resolution could make the signals much harder to detect. For this reason, a -6 dB width of around 1 mm was chosen as a compromise between signal power and resolution.

In order to have the desired spatial resolution, the tip of the probe needs to be thin. However, manufacturing and using such a thin probe would be very challenging. For this reason, a stepped design is used to achieve both high resolution at the tip and sturdiness at the base [39]. Stepped monopole design has been previously used to achieve better impedance and radiation characteristics [40], [41]. However, the choice of a stepped diameter design in our case is mostly for structural support. A 0.2 mm needle with a 1.27 mm handle is used for this purpose. Such needles of varying diameters can be found in the market as nozzle cleaners for 3D printers and airbrushes. The D_2 diameter is picked based on available needle sizes. This needle is then soldered onto an SMA connector and a PTFE sleeve of 4.1 mm is slipped on for added stability and miniaturization. D_3, diameter of the

PTFE is picked according to the diameter of SMA connector PTFE sleeves. Finally, the ground plane is screwed onto the connector. For this project, we limit the length of the tip of the needle to 4 mm; however, it is beneficial to leave it longer initially and slowly trim the length until the desired matching and coupling suppression is achieved on the VNA. The manufactured prototype can be seen in Figure 22.

It is also desirable to have low coupling between the transmit and receive probes. This would be difficult to implement if both probes were of the same type (i.e. both were monopole or coil). Coupling between the probes are mainly problematic because the injected carrier signal is much stronger than the received backscattered signal. If the very strong carrier couples to the receive probe, it can saturate the LNA, spectrum analyzer, software defined radio, or another type of receiver. The orthogonal nature of the monopole and the coil make it easier to realize this design goal.

4.3.2 Spatial Resolution, Isolation, and Invasiveness

The diameter of the probe tip has a large effect on the spatial resolution. Figure 23 (a) shows the change in the relative power on a plane 0.2 mm away from the probe tip for different tip thicknesses. It can be seen that the spatial resolution degraded by approximately 30% from 0.5 mm for a thickness of 0.4 mm as compared to 0.2 mm diameter, (indicated by two arrows in Figure 23 (a)). However, there is not much improvement in the resolution for further reducing the tip diameter beyond 0.2 mm.

An important consideration in proposed sensor geometry is how the combination influences the individual performance. Figure 23 (b) shows the effect of the multi-turn loop on the E Field probe resolution. Even though the addition of the multi-turn loop does widen

the pattern at few millimeters away from the center of the beam, the center of the pattern is relatively unchanged by the placement of the H field probe.

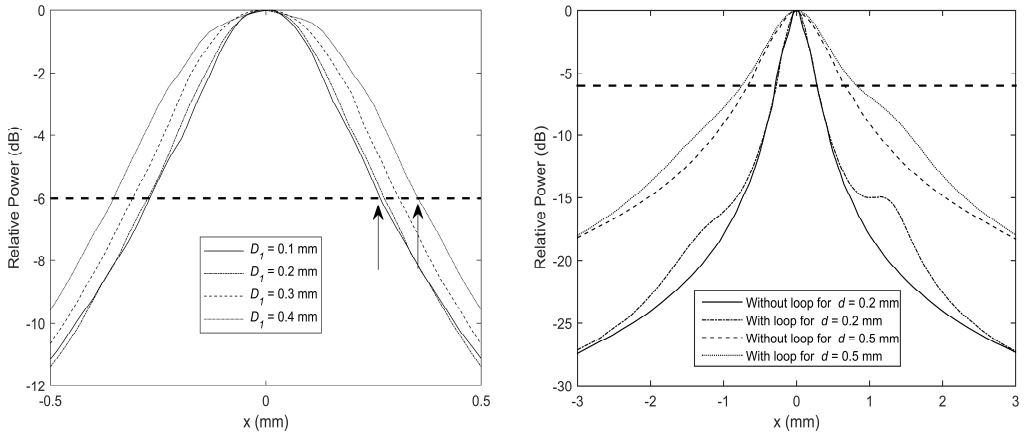
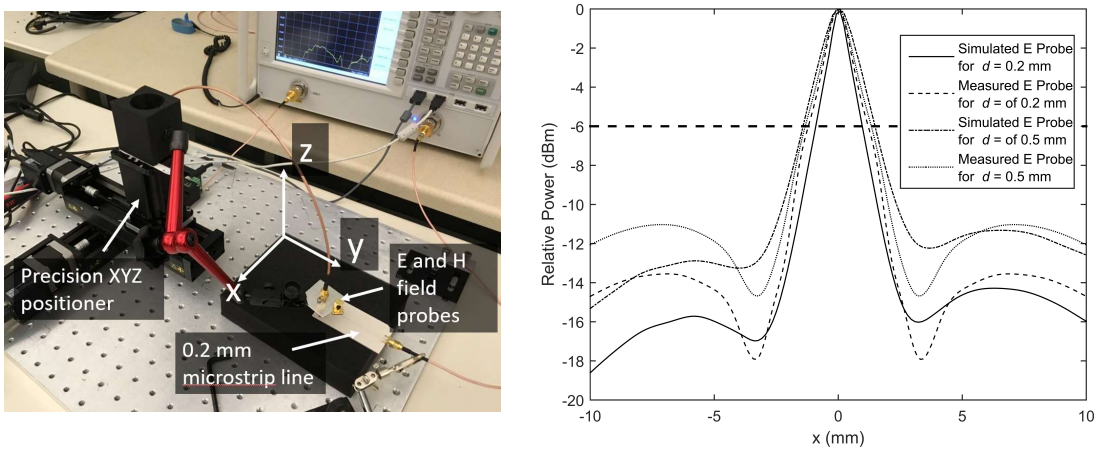


Figure 23 (a) Simulated effect of the E probe tip diameter on the spatial resolution for *d* = 0.2 mm. (b) Simulation of the effect of the presence of the H coil on the resolution of the E probe.

We use a VNA to measure the transmission between the E field probe and a 0.2 mm thick microstrip transmission line. We use a Zaber brand micron precision [42] positioner to scan the transmission line and obtain the S_{21} values as the probe passes over the transmission line for d = 0.2 mm and d = 0.5 mm.

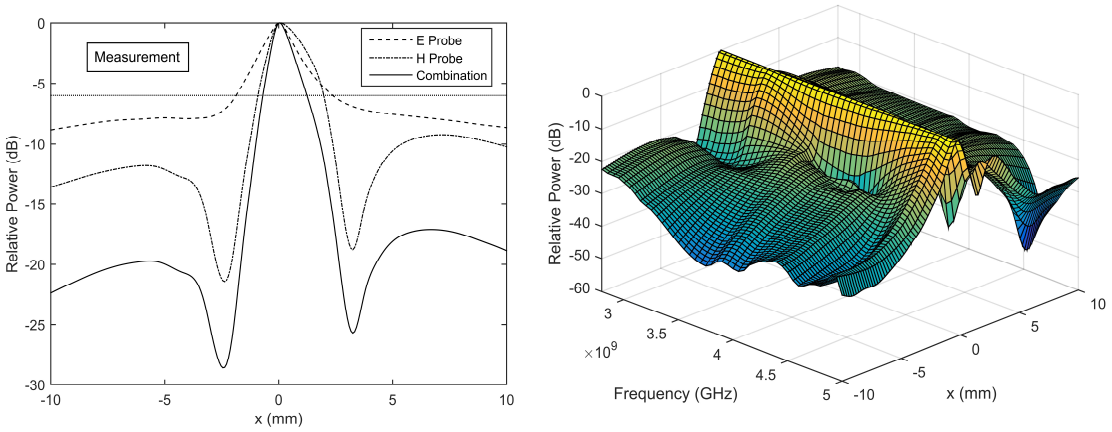
The microstrip line resolution measurement setup can be seen in Figure 24 (a). A precision positioning setup with 1 μm precision is used to hold the probe and it scans across a microstrip line of 0.2 mm width. One end of the microstrip line is connected to the VNA while the other end is terminated by the characteristic impedance of the line to eliminate variations in fields along the length of the microstrip. The other port of the VNA is connected to either E or H field probe while the other one is terminated by 50Ω. The measurement is repeated twice to get the result for both E and H field probes.



(a) (b)

Figure 24 (a) Positioner for the microstrip line measurement. (b) Simulation vs measurement comparison for the E Probe positioned at d = 0.2 mm and 0.5 mm.

Figure 24 (b) shows the comparison of the simulation and measurement results for the scan of a 0.2 mm thick microstrip transmission line. The measurements were repeated for d = 0.2 and 0.5 mm. Due to the mechanism of this backscattering application, the combined performance of the two probes is very crucial. The transmitter excites the spot region on FPGA according to the E field probe pattern and the receiver receives the fields according to the H field probe pattern. If there is a particular location on the FPGA where the E field probe excites 3 dB weaker than maximum and the H field probe receives 3 dB weaker than maximum, the total signal received from that location will be 6 dB weaker than maximum. In Figure 25 (a) the combined patters of the E and H field probes can be seen.



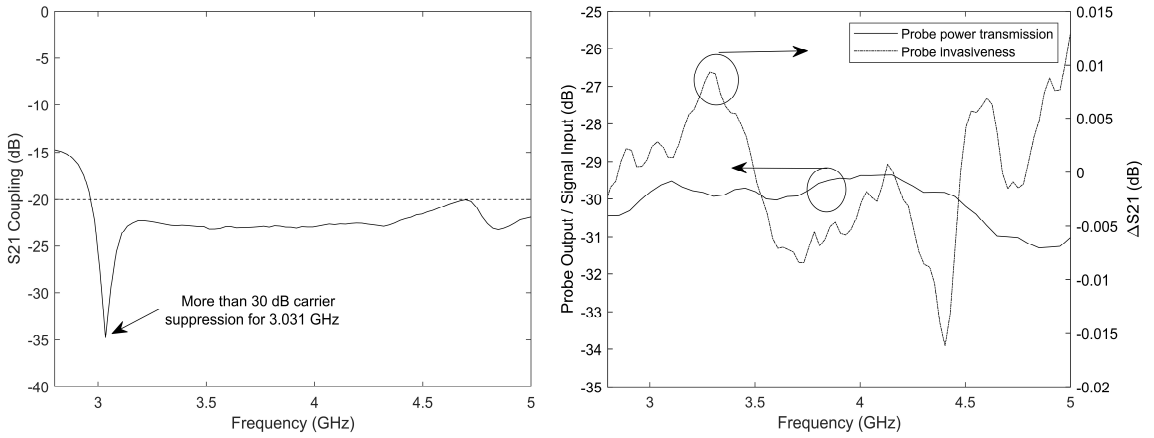
(a) (b)

Figure 25 (a) E and H Probe combination measurement at z = 0.2 mm. (b) The sensor relative power pattern performance up to 5 GHz.

This particular backscattering application is mostly done between 3 and 4 GHz; however, the pattern and the strength of the probe combination is viable in a greater range of frequencies. The pattern of the probe combination up to 5 GHz can be seen in Figure 25 (b).

As mentioned before, coupling can cause problems in this application. From Figure 26 (a), it can be seen that there is at least 15 dB suppression around the range of values that we use for the carrier and more than 30 dB suppression for the choice of carrier in this particular study (3.031 GHz).

Since the signals we are trying to detect are modulated and backscattered unintentionally, another important is the total signal strength. In Figure 26 (b) the total received signal strength is shown on the left axis, which is the S_{21} value for the transmission between the microstrip line and the probe. The probe has a relatively flat response between 2 and 5 GHz, and the tradeoff between the signal strength and resolution was suitable for our application.



(a) (b)

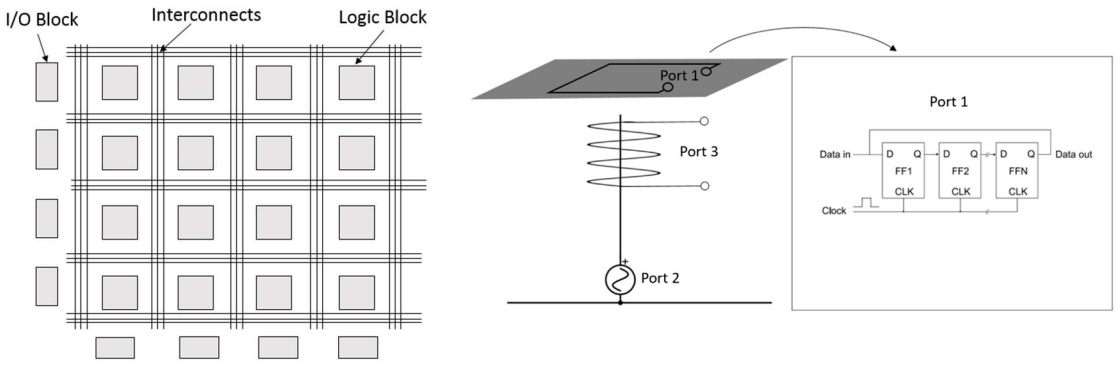
Figure 26 (a) The coupling between E and H field probes are lower than if both transmit and receive probes were of the same type. (b) The probe sensitivity and the invasiveness of the E field probe measured with the microstrip transmission line scan.

The other important consideration for our application is the invasiveness of the probe. It is undesirable to influence the FPGA circuit on the receive side. This shows the change in the S_{21} values on for the microstrip line when the E field probe is in close proximity (0.2 mm away) and completely removed. It can be seen that the impact of the probe on the working of the transmission line is less than 0.01 dB.

4.4 Near field Backscattering from FPGA: EM Circuit Co-Simulation

Backscattering from FPGA was shown in [1] for RFID applications. Two horn antennas were used as a transmitting and receiving antenna. It was shown that the incident wave from the transmitted antenna was modulated by an instruction in FPGA which has a simple combinational logic using NAND gates. Here, we have used a combination of grounded monopole and a short helix as a transmitting and receiving probes. Since the probes are in close vicinity of FPGA, possibility of near field backscattering is expected.

Figure 27 (a) shows the standard FPGA architecture having combinational logic, programmable switching block and I/O circuit. Near field backscattering from the FPGA surface can be explained using the backscattering from switching logic gates. The combinational block and the programmable switching block contain the combination of transistors. These transistors will switch between ON and OFF states corresponding to the instruction and the routing network in FPGA. To have a measure of the exact amount of the radiated backscattered power for a given instruction in FPGA, the full wave EM modeling of the transistor in the route are required. This can be cumbersome due to large number of transistors and due to simulations times. Instead of that, for explanation and for a proof of concept, we show the backscattered radiation from the power lines and the NAND gates in the logic blocks as shown in Figure 27 (a).



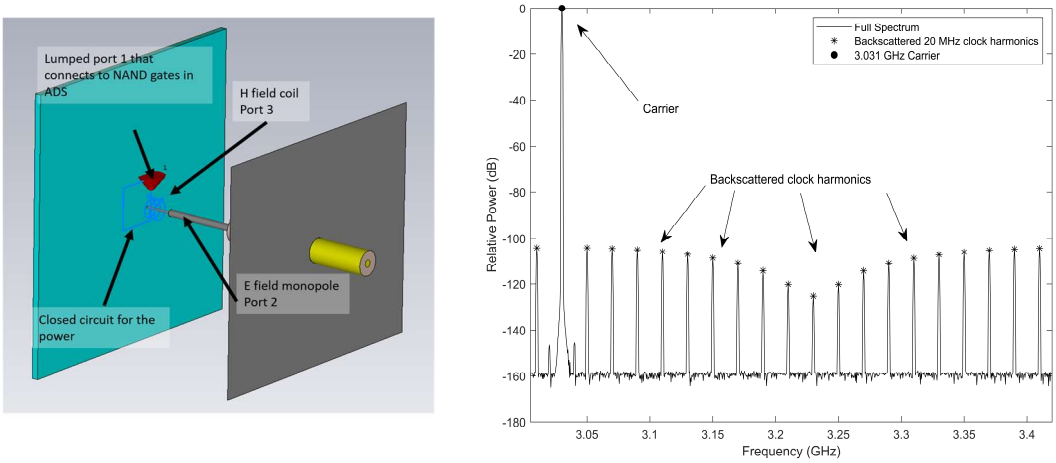
(a) (b)

Figure 27 (a) Internal architecture of an FPGA. (b) The switching circuit used in the CST simulations.

The combinational logic uses here is the simple flip flop, made of NAND gates, the standard logic building block of an FPGA. The diagram of the simulation setup is shown in Figure 27 (b). The electric monopole is excited by a signal source, a block that is containing the logic circuit is placed in close proximity, and the resulting signal is picked

up by the magnetic field probe. The 3D model including the E and H probe combination and a loop containing the switching element is shown in Figure 28 (a).

To further explain the near field backscattering from a switching circuit, EM-circuit co-simulations were performed using CST and ADS. In Figure 28 (a), the proposed monopole is used as a transmitting probe and the proposed coil is used as the receiving probe. The switching circuit here is represented by an electrically small single loop with a lumped port which is then connected to a series of NAND gates made up of BSIM CMOS transistor models in ADS. The spectrum of the received signal from the H probe is shown in Figure 28 (b).



(a) (b)

Figure 28 (a) The CST model showing the FPGA setup. (b) Carrier frequency of 3.03 GHz is modulated by the clock frequency of 20 MHz as simulated by CST and ADS.

4.5 Hardware Trojan detection using the backscattered signal

This section discusses the HT detection application of the proposed FPGA backscattering setup. Subsection 4.5.1 discusses the measurement setup and the received

modulated scattered signal that carriers the signature of the ~1 mm region of the FPGA under test. Subsection 4.5.2 evaluates such signals received from both HT-injected and HT-free circuits and compare them with a circuit known to be HT-free in order to detect signals coming from HT-injected circuits.

4.5.1 Near Field Backscattering

This section presents the measurement set up used for the near field backscattering. The FPGA measurement setup is shown in Figure 29. The FPGA is configured to run an Advanced Encryption Standard (AES) code. The E and H probe combination is positioned on the FPGA chip and the location is fine tuned to get maximum signal reception. As in Section 4.4, the E probe is excited by a 3.031 GHz carrier. There are several considerations for the choice of carrier frequency. The carrier must not be a multiple of the clock frequency because this could cause the modulated backscattered clock harmonics to overlap with the regular clock harmonics. The carrier should be chosen in a band where there would be minimal noise from the other board components such as voltage regulators, external ICs, etc. Finally, the carrier should be chosen to be at a frequency where there is minimal coupling.

As shown in Figure 26 (a), there is more than 30 dB isolation between the E and H probes, which help prevent the LNA and the spectrum analyzer from saturating.

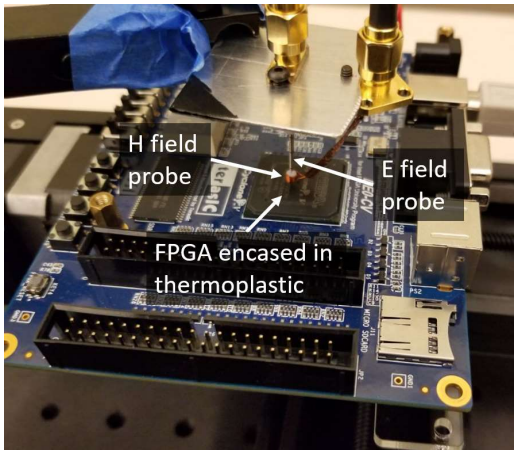


Figure 29 Positioning of the probe for the FPGA measurement setup.

A sample of the received spectrum from the H-field probe can be seen in Figure 30. The strongest peak is the carrier sent by the signal generator and the peaks marked with an asterisk are the backscattered 20 MHz clock harmonics that we are interested in. Since the mechanism of the phenomenon is the unintentional modulation caused by the switching transistors and logic gates, the modulated signal is quite weak and localized, which is why we need a good compromise between resolution and sensitivity and find a way to have both probes in very close proximity.

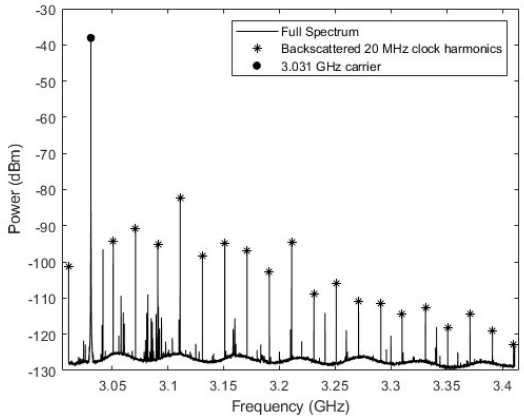


Figure 30 First 20 backscattered clock harmonics, measured with the proposed probe.

The particular values of the clock harmonics are what we are interested in. The configuration of the FPGA logic circuit has an influence on the power levels of these clock harmonics, meaning differences in the circuitry cause differences in the power levels of the harmonics. Conversely, a change in the levels of these clock harmonics indicate a change in the FPGA configuration. These differences can be detected and be considered an indication of intrusion.

The difference between clock harmonics are shown in Figure 31. To detect a tampering (hardware Trojan injection), we measure the first 34 clock harmonics 40 times and use this as the baseline. After the training round, we record the clock harmonics for HT-injected and HT-free cases 40 times each and compare the power levels with the training data set. In Figure 31, the power levels are similar for some harmonics but there are particular harmonics that differ significantly, namely the 8^{th} and 9^{th} harmonics. The 2 dB deviation from baseline in these two harmonics are sufficient to detect hardware Trojan with 100% success without false positive for a sample size of 40. This method applied successfully with different FPGA codes and different HT codes can be found in [12].

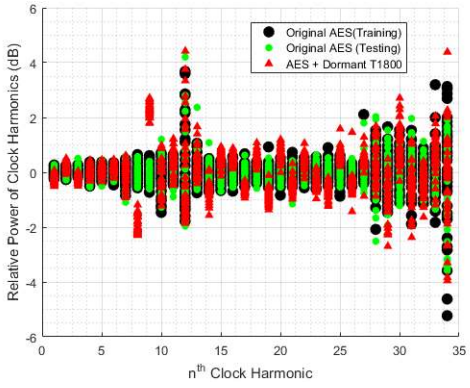


Figure 31 Amplitude ratios of the backscattered clock harmonics for HT-free and HT-injected FPGA's. Each data point is normalized to the mean of its HT-free measurement.

4.5.2 Conclusions

We presented a near field measurement setup and a novel sensor topology for exciting and measuring backscattered signals from a small spot of ~1 mm on an FPGA for HT detection. The sensor topology introduced utilizes a combination of E and H field probes in very close proximity. In this configuration, the E field probe is used to excite a carrier signal in the FPGA, and the H field probe is used to receive the modulated scattered signal that carries a signature of the tested logic circuit. To develop more understanding of how the injected signal may be modulated unintentionally to carry a signature of the circuit itself, an EM-circuit co-simulation was set up and analyzed. This modulated scattered signal was used in a HT detection scheme where all the HT-injected circuits were detected with no false positives. To better quantify the performance of the sensor topology, the effects of having E and H field probes in close proximity were assessed. The effects on resolution, mutual coupling, and invasiveness were examined and shown to have minimal drawbacks compared to the individual performance of the probes. It was found that the probe combination has a spot size of ~1 mm and a coupling isolation of better than 20 dB.

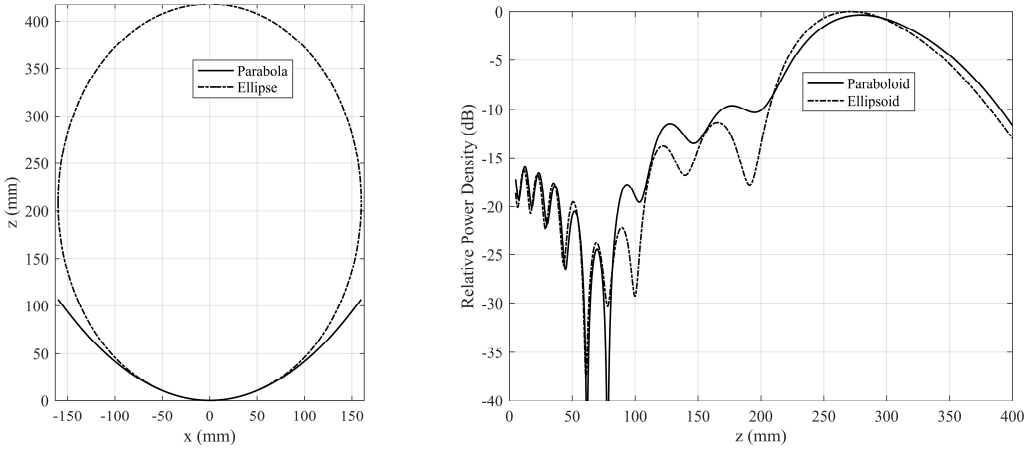
CHAPTER 5. THZ NEAR FIELD FOCUSING USING A 3D PRINTED CASSEGRAIN CONFIGURATION FOR BACKSCATTERED SIDE CHANNEL DETECTION

5.1 Overview

In this study, THz near field focusing is used for backscatter side channel detection. The frequency of operation was chosen as 300 GHz. This frequency offers a wide bandwidth, less interference from the environment, and a smaller focus spot. Near field focusing is done by using Cassegrain reflector configuration. The focuser is designed to produce the focused beam 28 cm away from the antenna aperture. The focusing is done in the near field region by axially moving the subreflector from the focal point. The focused antenna gain is 46 dBi while the 3 dB focus width and depth of the designed antenna is ~4 mm and ~10 cm, respectively. It is found that the focal plane position is sensitive to the subreflector shifts and effects of misalignment are studied. Simulations are compared with measurement results of a fabricated prototype and good agreement is observed. The antenna is fabricated by using 3D printing technology, which allows rapid and cheap prototyping. The surface is metalized using silver paint, the performance degradation due to the surface finish was analyzed and found to be minimal. Finally, we have demonstrated the detection of backscatter side channel from the board placed at 28 cm away from the designed antenna. The received power level of the backscatter signal increases by 6 dB as compared to horn antenna at a 6 times greater range.

5.2 Near field focused Antenna Design

This section presents the near field focusing using Cassegrain antenna system at 300 GHz. THz frequency focusing using a dual reflector offset configuration with an ellipsoidal main reflector was shown in [43] for imaging and scanning applications. In general, ellipsoidal reflector configurations have been widely used for near field focusing. In our case, we selected Cassegrain configuration with a paraboloid as main reflector since it can be easily converted into an optimal far field antenna (not discussed in this study) using struts of corresponding lengths. Also, for our case the main reflector size is 10 cm, for which the profiles of both elliptic and parabolic reflectors are approximately similar with a maximum difference of $\lambda/20$ at the edges. This is clearly shown in Figure 32 (a) where the equation of the parabolic profile (selected for design) is $z = x^2/240$ and the equivalent elliptic profile for similar near field focus location is $\frac{(z-209)^2}{(209)^2} + \frac{x^2}{(160)^2} = 1$.



(a) (b)

Figure 32 (a) Comparison of the parabolic and equivalent elliptic profile for main reflector. (b) Relative power density of the paraboloid reflector and the equivalent ellipsoid reflector

For larger main reflector sizes, say 30 cm, the two profiles are different at the edges; hence using a parabolic profile can affect the near field focusing parameters. To confirm, for a diameter of 10 cm, we performed full wave simulations with both paraboloid and equivalent ellipsoid profile as main reflectors (secondary reflector profile remains same). The relative power densities along z-axis is shown in Figure 32 (b). The maximum power density region has similar location (difference is < 3%) along the axis, for both the profiles. For paraboloid reflector, the maximum power density is 0.35 dB less than ellipsoid, which is acceptable in the present case as the parabolic configuration can be converted into far field antenna, with 0.35 dB more gain as compared to ellipsoid reflector.

The focusing antenna geometry is illustrated in Figure 33. For the side channel reception requirement, the focusing plane should be within the range of 25-35 cm from the antenna aperture. In other words, this represents the distance between the board or chip surface and the antenna aperture. Hence, focus depth of the designed antenna should be ∼10 cm. The chip surface on the board is a 2 cm × 2 cm square surface, the required focus width for the incident beam should be within 5 mm. This poses the limitation on the focus width. Ideally, the focal plane position of the focused antenna should coincide with the surface of the board. We started the design for the value of 28 cm (i.e. the focal plane is at a 28 cm distance from the subreflector, as shown in Figure 33)

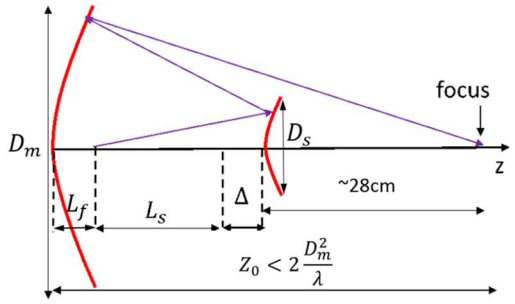


Figure 33 Illustration of near field focusing in Cassegrain configuration at 28 cm by shifting the subreflector from focal point by Δ.

It is well known that when the second focal point of subreflector overlaps with the focal point of the main reflector, the beam is focused at infinity (in the far field). To focus the beam at a finite distance in the near field region, the subreflector needs to be shifted axially along z-direction away from the main reflector by Δ, as shown in the Figure 33. This will result in focusing of the beam at Z_0, which is the distance from the main reflector vertex to the beam focus. Here, we choose the focal plane position to be 28 cm from the subreflector vertex and have main reflector size smaller than 10 cm × 10 cm × 10 cm (meaning the primary reflector diameter must be 10 cm). To focus the beam in the near field region, i.e. $Z_o < 2D_m^2/\lambda$, the feed should be displaced by more than $2(\mathrm{F/D_m})^2$ in wavelengths [44]. For the Cassegrain configuration, the focusing is done by displacing the subreflector along the axis. It is known that to focus the antenna, a symmetric quadratic phase is required at the aperture [45]. The technique of shifting the subreflector is a straightforward way of achieving the desired phase distribution on the reflector. Equation (5.1) and (5.2) describes the parabolic and hyperbolic profile of the primary and secondary reflector respectively.

$$z = \frac{x^2}{4f_m} \tag{5.1}$$

$$\frac{z^2}{a_s^2} - \frac{x^2}{b_s^2} = 1 \tag{5.2}$$

Eccentricity and the magnification factor of a farfield Cassegrain antenna is given in [46], where f_e is the focal length of the equivalent parabola, $2\psi_0$ is the subtended angle of the main reflector, and $2\theta_0$ is the effective subtended angle at the feed.

$$M = \frac{f_e}{f} \tag{5.3}$$

$$e = \frac{M+1}{M-1} \tag{5.4}$$

$$e = \frac{\sin\frac{1}{2}(\psi_0+\theta_0)}{\sin\frac{1}{2}(\psi_0-\theta_0)} \tag{5.5}$$

For the initial far-field design, the eccentricity and magnification are 1.63 and 4.2 respectively. For the near field design, the subreflector is shifted away from the focus by Δ, which results in a change in *M*. Equations (5.3)-(5.5) are defined for farfield Cassegrain reflectors. In case of a nearfield focus by shifting of the subreflector (without modifying the subreflector shape), due to a mismatch in foci locations, (5.3)-(5.5) will not give the correct magnification factor *M*. To calculate an accurate value of *M*, Gaussian optics can be used since the feed horn has a narrow beamwidth [47]. The dual reflector system in the near field focus configuration can be represented by two equivalent lenses as shown in Figure 34. The magnification factor *M* is then obtained as

$$M = \frac{|f|}{\sqrt{(z-f)^2+z_0^2}} \tag{6}$$

where z_0 is Rayleigh distance (equivalent of focus depth), and z is waist location (equivalent of focus location). The magnification factor was calculated using (5.6) and its variation with subreflector shift is discussed in Section 5.3.

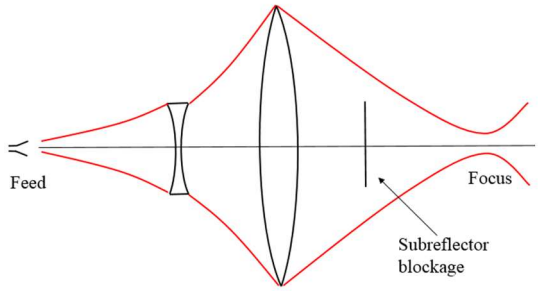


Figure 34 Equivalent lens configuration of the near-field focused Cassegrain dual reflector system.

The focus parameters are then calculated and compared with the full wave simulation results as shown in Figure 43 of section 5.3. The Cassegrain system was designed and simulated at 300 GHz using CST's Integral Equation Solver (version 2017) [48]. Initially the far field antenna having a gain of 46 dBi was designed. The geometrical parameters for the design are listed in Table I

Table I Design parameters for the 10 cm diameter paraboloid reflector antenna.

D_m	100 mm	Primary reflector diameter
f_m	60 mm	Primary reflector focal length
D_s	15.7 mm	Secondary reflector diameter
a_s	14.36 mm	Secondary reflector hyperbola parameter
b_s	18.48 mm	Secondary reflector hyperbola parameter
L_f	5 mm	Feed point offset w.r.t. primary reflector vertex
L_s	45.95 mm	Distance between the feed and the vertex of the secondary reflector
Δ	13 mm	Amount of shift applied to the secondary reflector to bring the focus to the nearfield

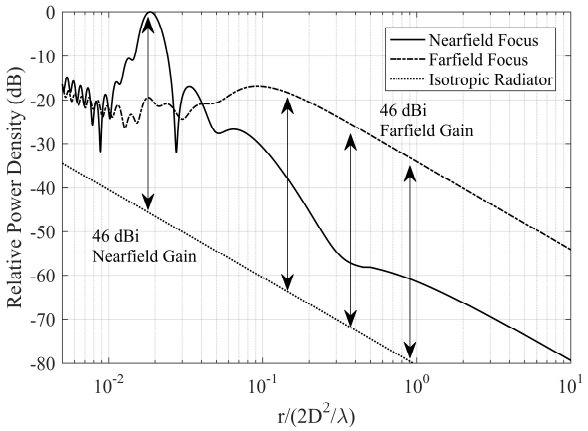


Figure 35 Relative power densities of near field and far field focused systems compared to the ideal isotropic radiator.

Near field focusing at the required position is then achieved by moving the subreflector along the axis. For the focal plane position to be at 28 cm from the subreflector vertex, the shift Δ is 13 mm. To show the near field focusing, the simulated power densities for the designed near field focus antenna and the far field antenna were plotted and shown in Figure 35. The power densities are plotted with the relative distance $^{r}/_{(2D_m^2/\lambda)}$ along the axis of the antenna. It is observed from the Figure 35 that for the far field antenna, the power density is 46 dB higher than the isotropic radiator at a distance of $2D_m^2/\lambda$. This is also expected as the initial far field antenna has 46 dBi gain. In contrast, the near field Cassegrain design has a very sharp peak in the near field. This peak is the focus of the designed antenna. Beyond this focal point, the power density decreases rapidly and falls below the power density of the far-field system as shown in the Figure 35.

In the far field dual reflector, the peak directivity value depends upon secondary illumination. For near field focusing, shifting of the subreflector will change the illumination and corresponding edge taper values. To check this, the simulated relative

power density vs the subreflector radius is shown in Figure 36. The power density is shown for both the initial far field configuration and the near field design. It is pointed out that the edge taper changes from 9 dB to 5.4 dB, as the subreflector is shifted to achieve near field focusing. This is a relatively low edge taper as compared to the conventional value of 10 dB. This is due to the mechanical consideration of having to mount the entire reflector on the body of the diagonal horn places constraints on the location and the size of the subreflector. For these reasons, the design was found to be a good balance.

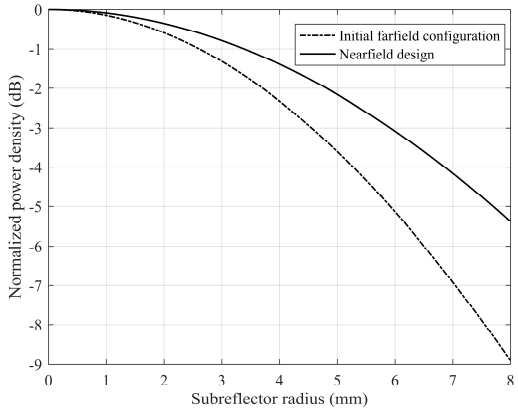


Figure 36 Normalized power density values vs subreflector radius for the farfield and nearfield configurations on the surface of the subreflector.

To investigate the different properties of the focus, in Figure 37 (a) we show the 2D power density plot in the yz-plane. The subreflector vertex is at z = 0 (i.e. the subreflector is placed between -1.2 mm < z < 0 mm, since the subreflector is 1.2 mm thick) and the y-axis shows the 10 cm region spanned by the width of the primary reflector. Figure 37 (a) shows that the field is weak and spread at z = 0 plane. However, as we move away from the subreflector, the field starts to concentrate around y = 0 and as it approaches the designed focal length of 28 cm, the field becomes very concentrated. Beyond this point,

the field spreads out again, losing its effectiveness as a near field focused antenna. The focus spot in the focal plane of the antenna (z = 28cm) is shown in Figure 37 (b).

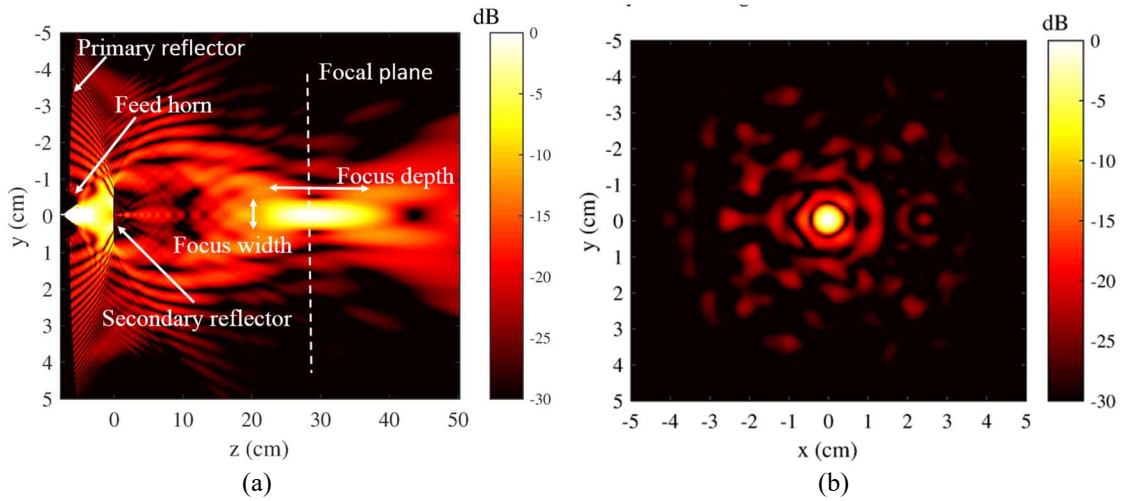


Figure 37 (a) Simulated 2D power density plot in yz-plane for the antenna geometry Focus sensitivity

5.2.1 Axial and lateral subreflector shift

The designed reflector was used in the application presented in section 5.5, which involves measuring of the power emanated by the board placed at a distance from the designed antenna. The measurement setup is shown in Figure 47 (a). It is well known from the previous studies that as feed moves along the axis the main beam can be focused at a finite distance. At THz frequency range, the operating wavelengths are few mm and a small deviation in the subreflector position from the designed value can affect the focal parameters. It is possible that this deviation can happen in the fabrication process. For this reason, in this section, we investigate in detail the sensitivity of the focus as a function of the position of the subreflector. The effect on various focus parameters such as focus width and depth, were investigated as the subreflector position changes. Along with the sensitivity, we also investigate the effect of the large subreflector shifts (up to 20 λ) on the

focus spot parameters. In the fabrication process, as explained later in 5.4.1, the subreflector is supported by the plastic struts (shown in Figure 46 (b)). The sensitivity of the focus is investigated by plotting a positional error of the location of the subreflector. Defining the position error δ (the axial offset of the subreflector in reference to the designed near field focused subreflector position, shown in Figure 38, where positive values of δ indicate a shift away from the main reflector), simulations were done for different δ values with a step size of 0.2 mm.

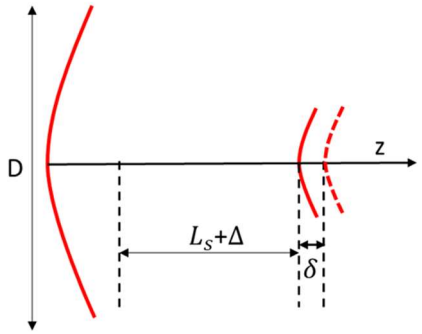


Figure 38 Geometry showing small shift in the positioning of the subreflector δ.

Figure 39 shows the change in the position of focus with the changes in the location of the subreflector. The manufactured prototype (corresponding to $\delta = 0$ mm) has a focal point at approximately 28 cm away from the antenna). As δ increases, the focal point moves closer to the antenna. As shown in the Figure 39, for 2 mm change in the position of subreflector, the focal point position changes by 44 mm. This shows that even a few mm deviation in the subreflector position will change the focal plane position. Although the fabrication and the measurement procedure has been discussed in detail in section 5.4, to validate the simulations, the measured position of the focus are also presented in the Figure 39.

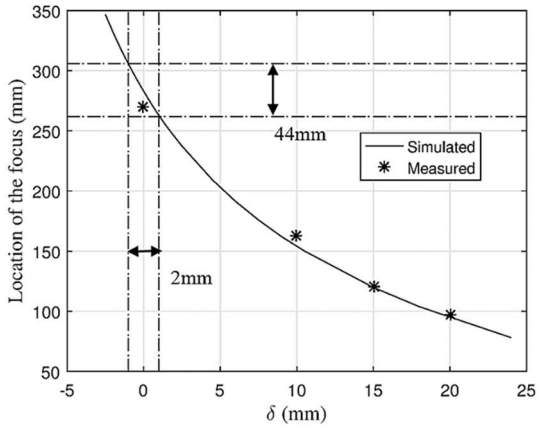


Figure 39 Location of focus vs subreflector shift.

We do not analyze δ values greater than 25 mm because the focusing performance of the antenna degrades quickly beyond that point. As shown in Figure 40, by increasing distance between reflector and subreflector by more than 25 mm, we start observing multiple focus points that are significantly weaker than a single focal point.

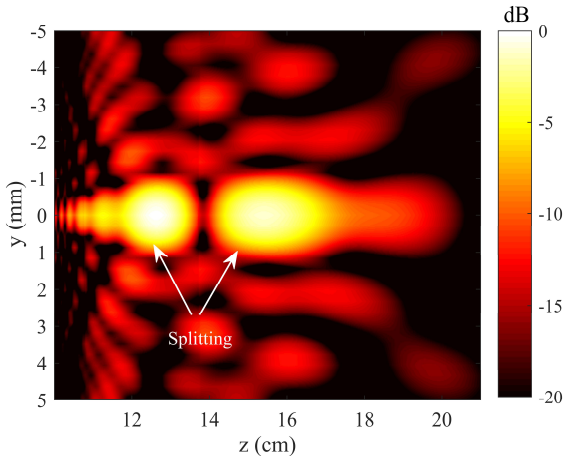


Figure 40 Focus splitting behavior beyond $\delta = 25$ mm.

For the EM side channel detection, presented later in section 5.5, the focus spot parameters like depth and width play a major role. Focus width, defined in the focal plane, will provide the information of how much area on a chip can be illuminated without the loss of power density. Focus depth on the other hand will provide the measure of the power

density variation in the axial direction, which is normal to the chip or board. To measure the focus spot parameters, we use a 3 dB cut-off compared to the point of the highest intensity. The focus width and depth refer to the focus dimension in the xy-plane and along z-axis, respectively. Focus width for the design is 4 mm. Figure 37 (a), show that the highest intensity region starts at about z = 25 cm and ends at z = 35 cm, giving us a focus depth of 10 cm.

The focus depth and width for different subreflector shift values are shown in Figure 41. It is found that a small shift in the position of the subreflector can have considerable impact on both of the focus parameters. In general, subreflector shifting along the z-axis reduces the size of the focus. Simulation results in Figure 41 show that focus width decreases from 4 mm to 2 mm as the subreflector shifts by 25 mm from the designed value. Similarly, for the same subreflector shifts, focus depth decreases from 100 mm to 20 mm. This implies that the minimum focus spot size is 2 by 20 mm.

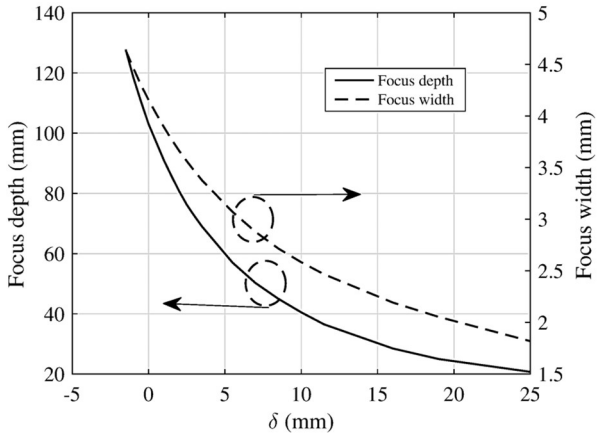


Figure 41 Simulated focus depth and focus width vs subreflector shift.

The focal parameters variation with subreflector shift can be explained using Gaussian optics as discussed in section 5.2. Figure 42 shows the magnification factor *M*

with subreflector shift. It can be seen that M decreases with δ and the lowest value converges to the far field configuration M of 4.3, which is close to the value obtain using (3). Figure 43 (a)-(c) compares the calculated values of focus parameters with the full wave simulations. It can be pointed out that for $\delta < 5$ mm, the calculated values provide good approximation of the focus.

One important factor that introduces inaccuracy to the calculation is the fact that the beam becomes too wide (in terms of angular spread) to be perfectly described by Gaussian optics upon reflecting from the subreflector. Another factor that is not taken into consideration is the calculations of the blockage caused by the subreflector, which degrades the depth and width of focus compared to the idealized Gaussian optics calculation.

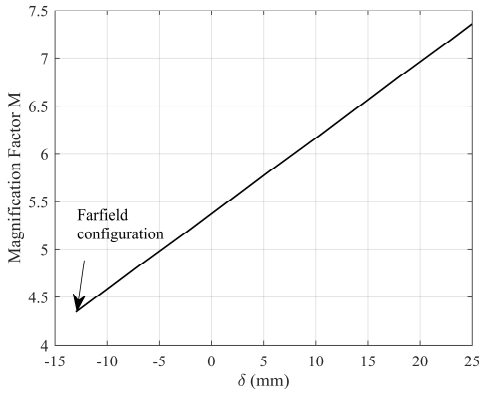


Figure 42 Magnification factor of the subreflector w.r.t δ.

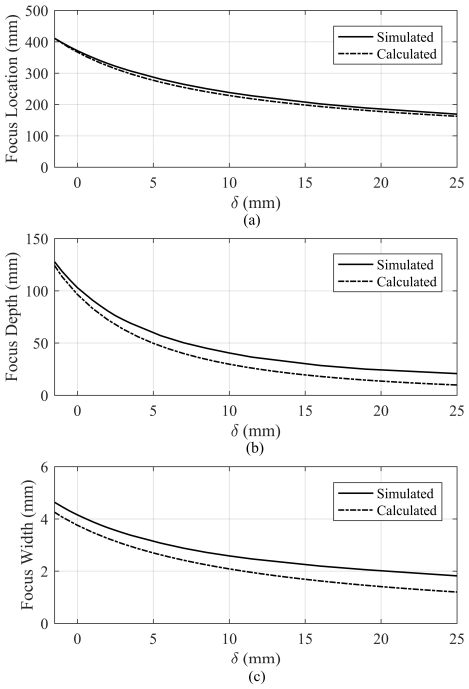
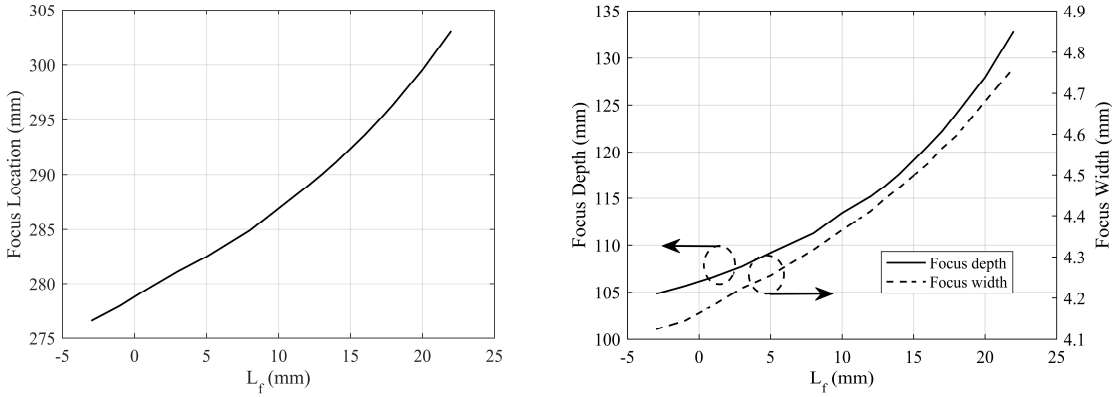


Figure 43 Comparison of simulated and calculated focus parameters based on Gaussian optics. (a) Focus Location, (b) Focus Depth, (c) Focus Width.

5.2.2 Effect of feed position

The feed position, L_f can affect the focus properties. The measurement setup limits the range of L_f as the length of the horn is 22 mm. Simulations were done for the different variation of L_f from its reference value of 5 mm and the effect on the focus properties were investigated. Figure 44 (a) shows the effect of feed position L_f on the focus location. Figure 44 (b) shows the effect of feed position on focus depth and width. Focus width changes by 0.6 mm and the depth changes by around 25 mm. The range of L_f in these plots are limited by the mechanical constraint of the total length of the horn, on which the reflector is mounted.



(a) (b)

Figure 44 (a) Focus location vs feed position L_f (default value is 5 mm). (b) Focus depth and focus width vs feed position L_f (default value is 5 mm).

5.2.3 Mutual Coupling Analysis

Since the feed horn use in the near field focused antenna design is high directive source, it is important to analyze the effect of mutual coupling between the horn and the reflector. Feed mismatch, Γ, can be calculated using the stationary phase method as given in [46] eq. (8-30) where ρ_0 is the distance to the vertex, $G_f(\rho_0)$ the feed gain in the direction of ρ_0, and ρ_1 and ρ_2 the radii of curvature of the reflector at ρ_0.

$$\Gamma = -j\frac{G_f(\rho_0)}{4k\rho_0}\sqrt{\frac{\rho_1\rho_2}{(\rho_1+\rho_0)(\rho_2+\rho_0)}}e^{-j2k\rho_0} \tag{5.7}$$

The feed receives the reflected power from the subreflector which results in the mismatch. The simulated reflection coefficient at 300 GHz, for the individual horn (without reflector) is -36 dB (0.016) as compared -26 dB (0.048), when it is used as a feed in the designed reflector antenna configuration.

The coupling effect is also observed in the aperture field of the horn feed. Figure 45 shows the electric field amplitude over the horn aperture. It can be seen that the aperture field is not changed significantly by the addition of the reflectors. The squared sum error of the entire field distribution is 0.05, which confirms that the mutual coupling does not have a significant effect on the aperture field distribution.

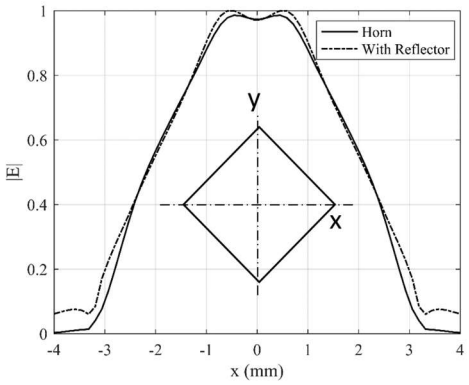


Figure 45 Simulated aperture field of the horn with and without reflector

The antenna geometry shown in the Figure 33 was designed, fabricated and tested. The antenna is fabricated using 3D printing technology. A type of nylon, PA2200, was used to fabricate the main reflector, the subreflector and the struts. The geometrical parameters for the fabrication have been listed in Table I.

5.2.4 Fabrication

The antenna has a main reflector and a small subreflector, which can be fabricated using lathe. Here, instead of that we used 3D printing technique for the fabrication of both the reflectors and struts. 3D printing allows for a cheap and fast prototype manufacturing that is precise and easy to modify. Below, we explain how the 3D printed plastic is treated to function as a metallic reflector.

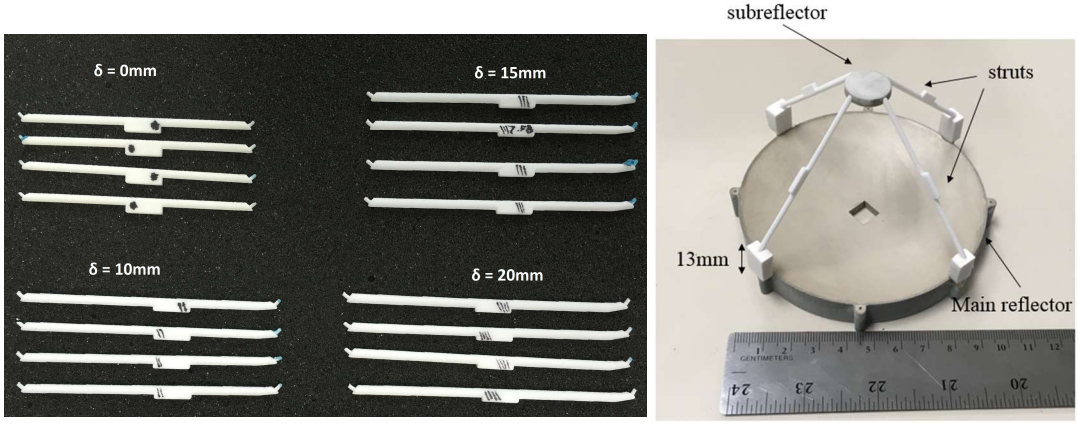
3D printers slice the model into thin stacked layers along the z-axis. Therefore, an important measure of quality for 3D printing is the layer thickness. Since curved features along the z-axis will show a staircase approximation in the finished prototype, working with smaller layer thickness will results in a more accurate product. The printer that was used, FORMIGA P 110, has a layer thickness of 0.06 mm, which would be very accurate for the lower end of the mm-wave range. However, for the THz frequency range operation (300 GHz), small imperfections on the reflector surfaces lead to phase error losses and can significantly affects the performance parameters like focused directivity. For this reason, additional smoothing had to be applied to the surface of the reflectors.

Prior to smoothing the surface by sanding, a thin single coat of a wet sandable automobile primer was applied to the surface. This primer provides a surface that is easier to smooth, and easier for the conductive paint to adhere to. After that, the surface was smoothed using first 600 then 1200 grit sanders. It is very important to use gentle methods or instruments in this process so as not to change the geometry of the reflector and only remove the nonidealities of the printer.

The smoothed surface becomes ready for the conductive paint to be applied. The particular conductive paint that was used here is MG Chemicals silver paint. There are many different brands of conductive paints with several methods of application. The most convenient products would be aerosol cans; however, for this prototype 0.2 mm nozzle airbrush was used to spray pure silver paint on the prototype at a 20 cm distance to get uniform coating. This method allows for greater control over how the paint is dispersed and ensures the best quality of surface conductivity. The outlined method resulted in a

conductive surface that very well matched the simulations using perfectly smooth PEC surfaces.

The second significant design choice was the struts. For this prototype, four replaceable struts were used to suspend the subreflector. The greatest benefit of these struts is that different sets of struts can be used to hold the subreflector at varying distances away from the subreflector. The same reflector system can switch from a far field antenna configuration to a near field focus configuration manually in under a minute. Moreover, struts of varying lengths can be used to further tune the location of the near field focus as shown in Figure 41, a technique that was used in this paper. We have manufactured three different lengths of struts as shown in Figure 46 (a). Some applications could potentially utilize asymmetrical struts to hold the subreflector at an angle to change the beam direction, but this was not investigated in this paper.



(a) (b)

Figure 46 (a) Sets of struts of different sizes. (b) The silver coated and assembled reflector (without feedhorn).

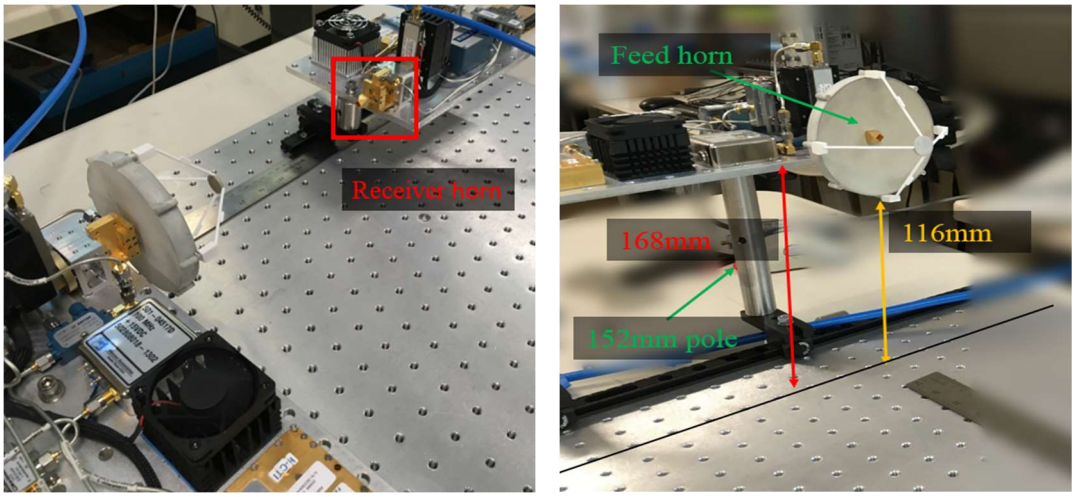
There are many other ways to suspend a subreflector in front of a main reflector. The fact that the reflector system can be easily assembled and disassembled becomes very

convenient when the reflector surfaces are smoothed and painted. If the entire reflector system was a single piece, the pieces would have been more rigidly aligned (e.g. if replaceable struts are used in a vibrating system, the alignment might degrade as time goes on); however, the reflector surfaces would be much more difficult to reach for even smoothing and painting. The main reflector has a 9 mm square hole in it to fit onto a diagonal feed horn of the measurement system. The reflector can be used with a less or more directive feeds; all that is necessary is to adjust the square hole size in the main reflector so that it will fit securely onto the feed-horn. The final form of the reflector is show in Figure 46 (b).

5.2.5 Measurements

The measurement setup consists of the N5224A vector network analyzer (VNA), the VDI transmitter (Tx210), and the VDI receiver (Rx148). In the transmitter, the THz-range carrier signal starts out as a 25 GHz signal, which is generated by a Herley-CTI phase-locked dielectric resonator [49]. This signal is amplified, and its frequency is doubled using Norden N08-1975 [50]; and then, its frequency is tripled using VDI WR6.5X3 [51].This signal is then fed to a subharmonic mixer (WR2.8SHM [52]) that plays a dual role of doubling the carrier frequency and mixing it with the baseband input signal (delivered by the VNA). The THz-range signal is then transmitted by the horn antenna that has a gain of 25 dBi in the range of operation. At the receiver side, the same components are used to downconvert the signal. The final signal is fed back to the VNA and the transfer parameter S_{21} results are calibrated. The measurement section in [53] describes the Tx-Rx system in even more detail. The transceiver system with the designed antenna on transmitter and horn on the receiver is shown in Figure 47 (a). This system was then placed

on a perpendicular set of dovetail optical rails on an optical breadboard to cover the entire 2D plane. The system was elevated from the ground plane (the optical breadboard) using 25.4 mm and 152.4 mm poles as shown in Figure 47 (b).



(a) (b)

Figure 47 (a) The Tx-Rx system with the reflector on the Tx side. (b) Height of the focusing antenna from the ground plane.

The designed reflector itself has a very wide bandwidth, for this reason its frequency performance parameters are only affected by the feed diagonal horn and the transmitter. The bandwidth of the diagonal horn is 260 GHz - 400 GHz and the bandwidth of the transmitter is 300 GHz – 320 GHz.

Proximity of the antennas to the ground plane is not a concern in this setup as the focused beam has narrow first null beamwidth and hence will not reflect from the ground for the given heights used in measurements. This has been thoroughly validated by measurements. In addition, there is negligible difference between an elevation of 25.4 mm and 152.4 mm. Measurements were done along the axial coordinate, which is the z-axis, and in the transverse xy-plane (focal plane). As shown in Figure 46 (a), struts of

different lengths were fabricated. These struts can be swapped to fine tune δ, the relative position of the subreflector. From the study done in the previous section, the location and the size of the focus is sensitive to δ, and hence experimental validation for different values is meaningful.

First, the relative power density was measured in the focal plane to check the focal spot width. The relative power density in the focal plane is shown in the Figure 48. The measured focus width (3 dB width) is around 4 mm, as shown in the Figure 48.

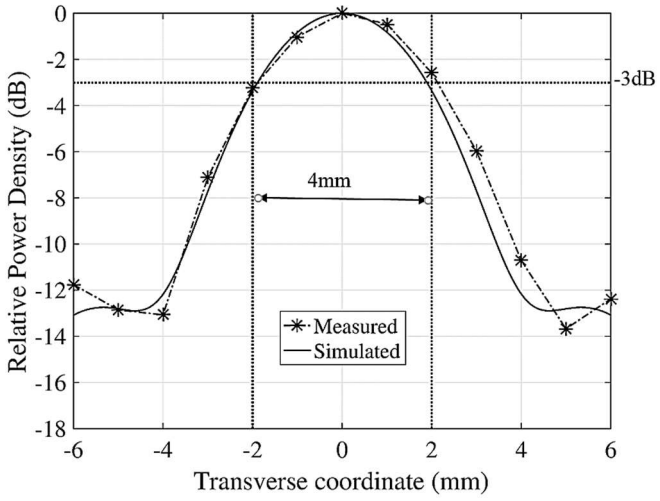


Figure 48 Relative power density in the focal plane.

Figure 49 shows the simulated and the measured power density of the designed antenna along its axis. In these plots, separation distance d is the axial distance measured from the secondary reflector, which is located at (0,0). Measured results agree very well with the simulated results. Upon de-embedding the losses in the cables and the transceiver system, we observe ~0.7 dB which is the result of the nylon struts, conductor loss, and the surface roughness loss of the silver paint. The loss analysis is discussed in detail, later in 5.4.3. Figure 49 (a) shows that for $\delta =$ 0 mm, the 3 dB focus depth is

97 mm, with maximum at 27 cm. Upon moving the subreflector 10 mm, i.e for δ= 10 mm, the focus depth reduces to 39 mm and the position of the maximum moves 11 cm closer. Similarly For δ = 15 mm and 20 mm; the focus depth reduces to 30 mm and 25 mm respectively; maximum moves 15 cm and 18 cm closer respectively.

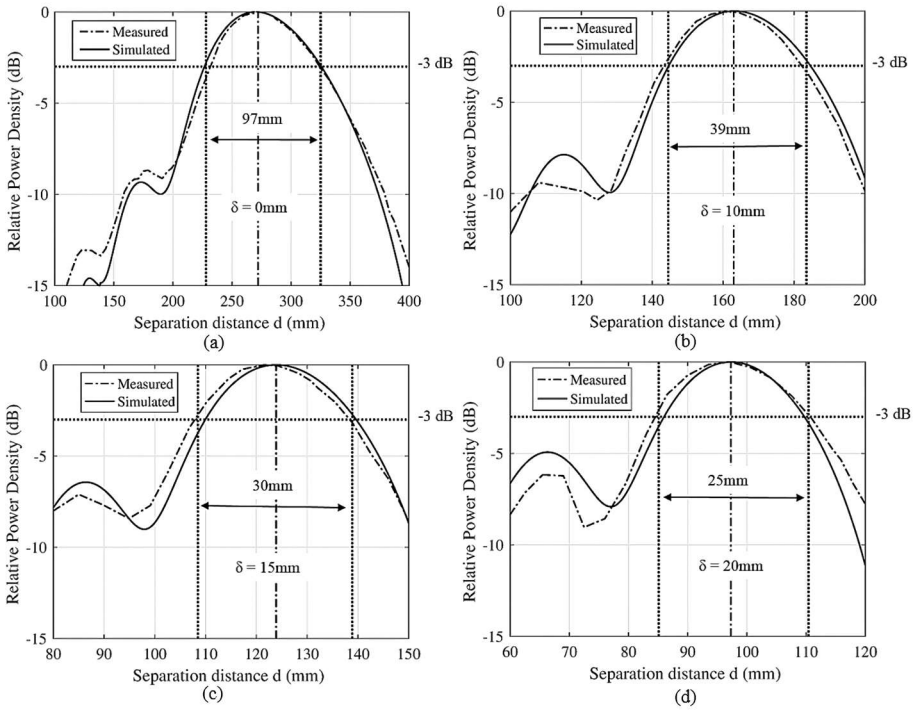


Figure 49 Simulated and measure relative power density of the prototype along the z-axis. (a) $\delta = 0\ mm$, (b) $\delta = 10\ mm$, (c) $\delta = 15\ mm$, (d) $\delta = 20\ mm$.

To evaluate the overall performance of the nearfield focuser, we use the focus antenna gain, similar to the focus antenna directivity defined in [54]. This parameter essentially compares the field intensity of the near field focused antenna at the exact location of the focus to the field intensity an isotropic source would have created at the same distance. In other words, the field created by our reflector antenna at a distance of 28 cm is 46 dB stronger than the field created by an isotropic source at a distance of 28 cm.

This is further validated with a gain transfer measurement using 2 identical horn antennas with 25 dBi gain. S_{21} power transmission with a separation distance of 28 cm was observed to be 21 dB stronger for Reflector-to-Horn setup compared to the Horn-to-Horn setup. This is also confirmed by the side channel detection measurements shown in the next section.

5.2.6 Loss analysis

At THz frequencies, the primary contributor to the loss in the antenna configuration is caused by surface roughness of the conducting material used in the fabrication. The roughness loss depends upon the variation in surface height. In practice, standard smoothing techniques such as polishing can be applied to minimize this loss. Figure 50 shows simulated and theoretical roughness loss w.r.t standard deviation of surface height for the designed reflector antenna. The theoretical loss is calculated using (5.8) [55].

$$\exp\left[-\left(\frac{4\pi\sigma_s}{\lambda}\right)^2\right] \tag{5.8}$$

The fabricated prototype was measured to have an RMS surface roughness of 4 μm, which results in less than 0.1 dB loss.

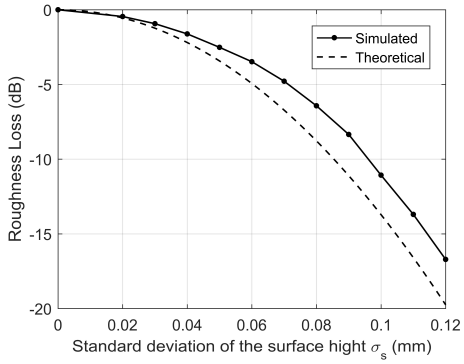


Figure 50 Loss due to the roughness of the surface.

Another source of loss is the imperfect conductivity of the silver paint. The effect conductivity has on the loss is shown in Figure 51. The datasheet for the MG Chemicals Liquid silver paint, used in prototype, has a conductivity value of 0.5 MS/m, which results in 0.15 dB loss.

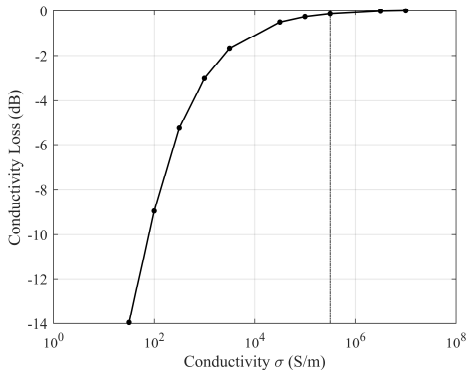


Figure 51 Simulated loss due to the conductivity of the paint.

Struts loss in investigated for the different struts size and is shown in Figure 52. For the fabricated prototype the struts diameter of 1.5 mm is selected, which results in 0.3 dB loss.

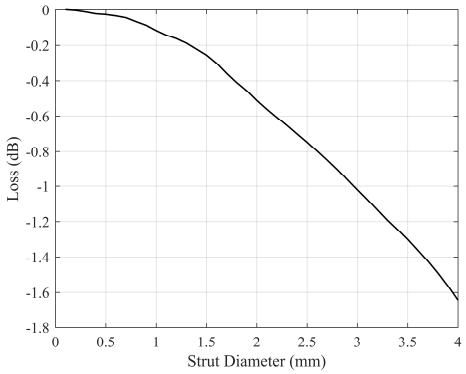


Figure 52 Simulated loss due to the obstruction of the struts.

Measurements shows 0.7 dB total loss compared to the ideal PEC Cassegrain; which is a contribution of surface roughness, conductivity and strut losses. The remaining 0.7 - 0.5 = 0.2 dB is likely a result of measurement uncertainty and miniscule imperfections in alignment.

5.3 Near Field Focuser in Backscatter Side channel Application

In this section, we conduct backscatter side channel measurements to demonstrate the performance of our proposed THz near field focuser. The goals are to show that the proposed near field focuser can effectively amplify the received backscatter signal and increase distance range, which are of critical importance due to THz (300 GHz) signal's high attenuation with distance. The backscatter side channel is created by switching activity of transistors in digital electronic circuits, such as microprocessors [1]. We have implemented a four-bit RFID design as described in [1] in Altera DE0-Cyclone V FPGA, and demonstrated that the message can be read from outside of the FPGA board via backscatter side channel. Details of circuit designs can be found in [1].

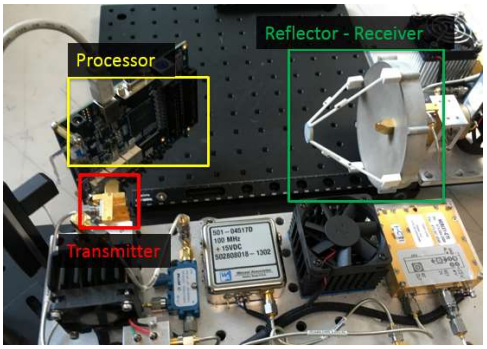


Figure 53 Backscatter measurement setup.

Figure 53 presents our backscatter measurement setup. An Agilent MXG N5183A Signal Generator with input power of 15 dBm is used as a signal source and an Agilent MXA N9020A Vector Signal Analyzer is used to record the backscatter signals. An Altera DE0-Cyclone V FPGA board is used as an electronic device that generates backscatter side channel.

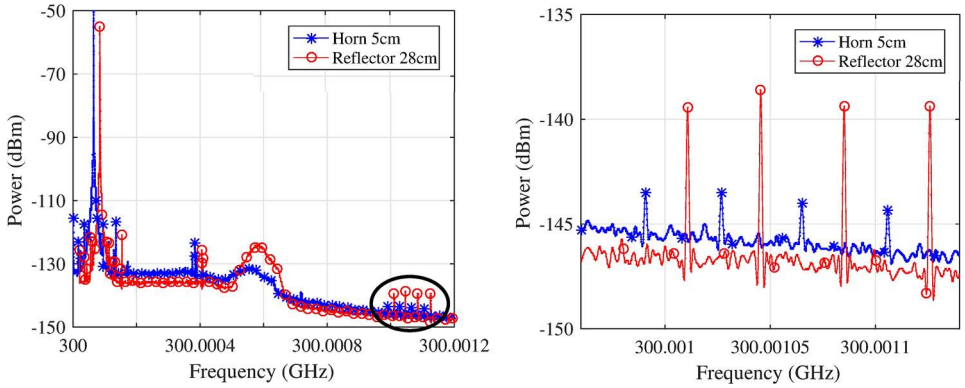


Figure 54 (a) Measured spectrums of the 4 bits backscatter signals at 300 GHz. (b) Measured spectrums of the 4 bits backscatter signals at 300 GHz; zoom-in of the modulated signals.

Figure 54 (a) presents the measured spectrum of the 4 bits backscatter signal at 300 GHz. The blue curve is the measurement result with standard gain horn antennas at a Tx-Rx distance of 5 cm and the red curve is the measurement result with the near field focuser

at a Tx-Rx distance of 28 cm. A relatively strong carrier signal is observed at around 300 GHz and all four modulated backscattered peaks are observed at around 1 MHz away from the carrier frequency. Note that a hump at around 600 kHz away from the carrier frequency is observed in Figure 54 (a). This hump is caused by the THz transceivers, which is not of interests in this paper.

Figure 54 (b) shows a closer look at the modulated backscatter signals. It is observed that the received backscattered power with the near field focuser is around 6 dB stronger than the power without the near field focuser at a distance that is almost six times farther (28 cm versus 5 cm). This means the reflector overcomes the extra 15 dB pathloss (28 cm vs 5 cm separation distance) and still delivers 6 dB more power. These power levels further validate our measured focused antenna gain value of 46 dBi. This is explained as follows:

$$\text{Increase in received power} + \text{Path loss difference} + \text{Gain of the feed horn} = \text{Focused Antenna Gain}$$

$$6\ \text{dB} + 15\ \text{dB} + 25\ \text{dBi} = 46\ \text{dBi}$$

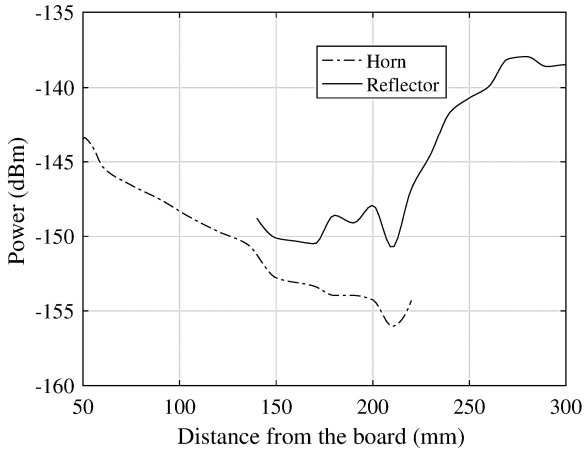


Figure 55 Received backscattered power level with respect to the Rx-to-FPGA board distance.

In Figure 55 we compare the averaged received power levels of a single bit obtained from the horn antenna and the manufactured reflector at distances from around 5 cm to 30 cm. It is observed that with the use of the horn antenna, the received backscattered power (dotted curve in Figure 55) gradually decreases as distance increases from 5 cm to 22 cm. At distance beyond 22 cm, the backscattered signal is no longer observable since it decays below the noise floor. In contrast, with the near field reflector, the received power (solid curve in Figure 55) reaches a maximum value at around -138 dBm as distance approaches 28 cm.

5.4 Conclusion

Backscatter side channel detection using THz near field focusing was presented in this paper. THz near field focusing allows the backscatter signal to detect at larger distances as compared to the far field radiator. The Cassegrain reflector configuration was used to design the focused antenna. The sensitivity of the focus parameters like focus depth and width w.r.t. the subreflector small shifts were investigated. It is found that 1 mm change in

the subreflector position can shift the focal plane by 2 cm. The relative power density along the axis for the various struts sizes were studied and it is found that the 3 dB focus depth decreases with increase in struts size. The focused antenna was fabricated using 3D printing technology, which facilitates rapid prototyping. Metallization of the reflector surfaces were done using conductive silver paint. Finally, we presented the backscatter signal detection using the designed antenna and it was shown that the designed antenna can detect the signal 28 cm farther from the board aperture as compare to the far field antenna.

CHAPTER 6. THZ BACKSCATTER SIDE CHANNEL SENSING AT A DISTANCE

6.1 Overview

This study presents the sensing and detection of backscattered THz side channels unintentionally created by FPGA activity and the focusing structures that are built for this purpose. At first, a single frequency is modulated onto a THz carrier due to the switching activity inside the FPGA and this modulated frequency is received at a distance. The effects of polarization and the receiver distance on the backscattered signal are studied and it is found that deliberately introducing a polarization mismatch between the transmitter and the receiver can improve the signal to noise ratio (SNR) by more than 10 dB. This allows the signal to be received at distances greater than 45 cm with an SNR above 54 dB, making detection feasible at several meters away. Through the use of a near field focuser, the properties of the side channel signal are measured over the surface of the FPGA board with a resolution of 0.5 mm. Next, backscatter signal at 4 distinct frequencies is created and detected through splitting the FPGA into 4 distinct modules. The relative strength of the frequencies is compared and conclusions about the physical location and the strength of these signals originating from distinct modules are analyzed. It is found that by focusing the backscatter system on certain locations on the FPGA can preferentially receive the signal from one module while filtering out the other modules. This helps isolating the signals created by various modules in an FPGA and significantly improving the effectiveness of side channel detection techniques. Finally, a 20 cm reflector is designed

manufactured and tested to receive the described backscattered side channel signals at ranges beyond a meter with high SNR.

6.2 ELLIPSOIDAL REFLECTOR DESIGN

The application detailed in this study imposes some requirements on the antennas. Due to the low signal levels caused by the nature of side channels, it is desirable to have a very intense focus to make up for the otherwise weak signals. Due to the possible spatial signal variations that are given off by the FPGA, it is desirable to have a small focus spot that would allow for the level of resolution that can distinguish interesting signal variations. For this purpose, an ellipsoidal reflector fed by a horn antenna is designed to create a near field focus from the transmitter side to excite the carrier of the backscattering scheme. This section presents the parameters and constraints of the reflector design. The primary considerations are the focus size (resolution) and focus intensity. Focus size needs to be small enough (in this case, limited to 1 mm) to resolve variation in the signal levels emanating from the FPGA. The focus intensity also needs to be high enough to detect these inherently weak signals since at THz frequencies the path loss is higher compared to lower frequency ranges. Based on the required focal spot size, the initial geometrical parameters of the ellipsoid were selected. The diffraction-limited resolution can be derived by modifying Abbe's criterion as shown in [56]. In the transverse direction (xy-plane), the spatial resolution can be approximated by [57]

$$\Delta y \approx \frac{0.82\,\lambda}{\sqrt{2}\,\mathrm{NA}} \tag{6.1}$$

where λ is the wavelength and NA is the numerical aperture. The resolution in the axial direction (z-axis) can be approximated as

$$\Delta z \approx \frac{4.4\,\lambda}{2\pi\,(\mathrm{NA})^2} \tag{6.2}$$

The numerical aperture in (6.1) and (6.2) is 0.89 for the model shown in Figure 56. To achieve the desired focus at 300 GHz, an ellipsoidal main reflector with a hyperboloidal subreflector fed by a 25 dBi diagonal horn, was designed and simulated. Simulation has been done in CST. A 3D model is shown in the Figure 56.

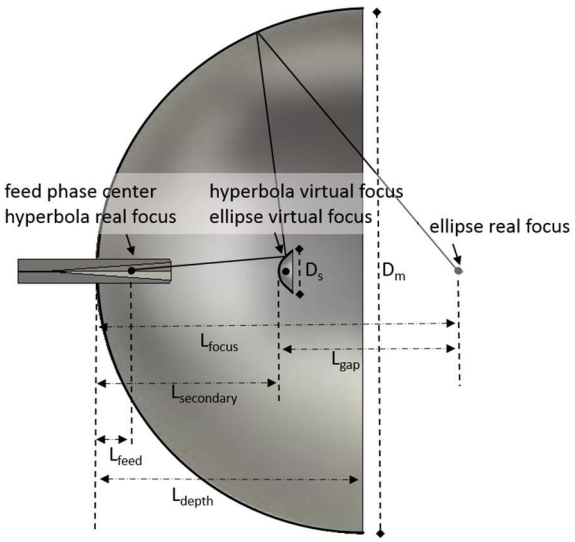


Figure 56 The nearfield focuser CST model.

Table 3 Design parameters (in mm) for the ellipsoidal reflector in Figure 56.

$\mathbf{D_m}$	190	Main reflector diameter
$\mathbf{a_m}$	100	Main reflector - ellipse parameter
$\mathbf{b_m}$	95	Main reflector - ellipse parameter
$\mathbf{L_{depth}}$	96	Main reflector depth
$\mathbf{D_s}$	16	Secondary reflector diameter
$\mathbf{a_s}$	25	Secondary reflector - hyperbola parameter
$\mathbf{b_s}$	12	Secondary reflector - hyperbola parameter
$\mathbf{L_{feed}}$	13.3	Feed point offset wrt. main reflector vertex
$\mathbf{L_{secondary}}$	45.95	Distance between the vertices of the main and the secondary reflectors
$\mathbf{L_{focus}}$	131	Distance between main reflector vertex and the focus
$\mathbf{L_{gap}}$	35	Separation between the aperture of the main reflector and the focus

$$\frac{z^2}{a_m^2} + \frac{y^2}{b_m^2} = 1 \tag{6.3}$$

$$\frac{z^2}{a_s^2} - \frac{y^2}{b_s^2} = 1 \tag{6.4}$$

Equation (6.3) describes the elliptical profile of the main reflector and (6.4) describes the hyperbolic profile of the secondary reflector. The numerical values and the descriptions of the parameters used in this design are shown in Table .

Figure 57 (a) shows the 2-D relative power density plot in yz-plane. The primary reflector is fed by the hyperboloid sub-reflector, which is in turn directly fed by the feed horn. The wave fronts converge at the desired focal spot. The wave front diverges quickly beyond the focal plane, as shown in Figure 57 (a), which is desirable. Figure 57 (b) show the power density in the focus spot region highlighted by the circle in Figure 57 (a). The simulated full width at half maximum (FWHM) values of the focus are 1.5mm for Δz (focus depth) and 0.7mm for Δy (focus width) which are within 10% of the theoretical formulas given in (1) and (2). The 3dB and 10dB contour lines of the focus is also indicated in Figure 57 (b).

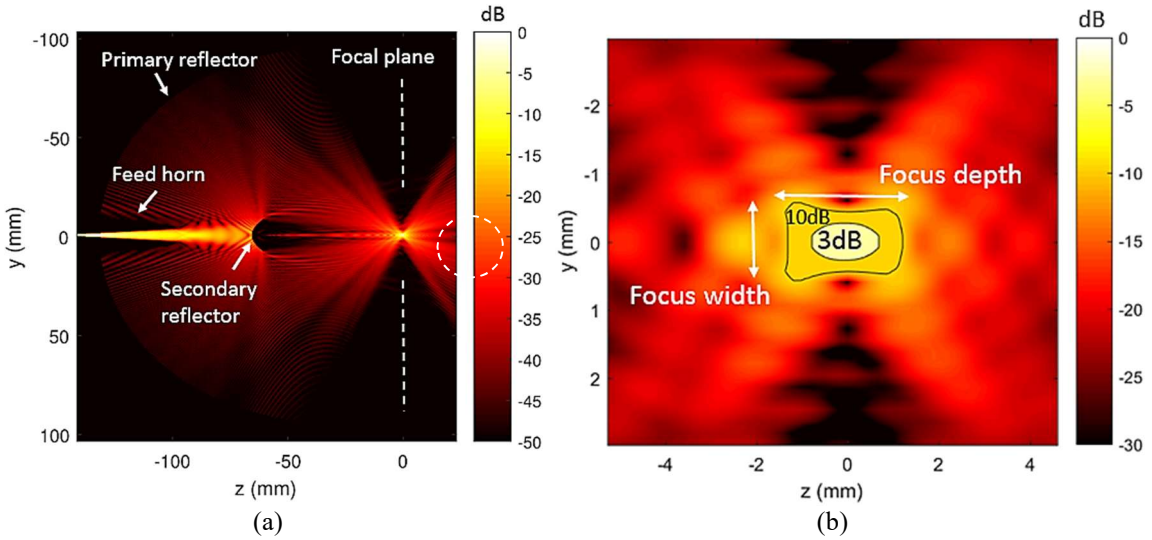


Figure 57 (a) 2D Relative power density plot of the reflector model shown in Figure 56. (b) 2D Relative power density plot on the focal spot region

6.3 THz Side channel Sensing: EM-Circuit Simulation

This section presents an EM-circuit co-simulation model and analysis for sensing of backscattered side channels from digital circuits at 300 GHz and its effect of polarization. We propose a proof of concept simulation for this phenomenon of unintentional modulation and polarization at 300 GHz. The goal here is to draw a distinction between the factors that are affected by linear scattering parameters of the 3D EM configuration and the nonlinear modulation effects that are caused by the switching elements in the FPGA circuit. There is no surprise that modulation happens through this mechanism, any nonlinear element can create some unintentional modulation. This simulation configuration will examine what factors play the key roles and if the modulation is strong enough to be sensed and detected at a distance.

In the EM simulation model, a 25 dBi diagonal horn is used on the transmitter side with the 20 cm diameter near field reflector focuser with an elliptical profile that creates a

focus 35 mm away from the aperture of the main reflector as explained in the previous section. This reflector system illuminates the FPGA with a 3 dB spot diameter of 0.7 mm. Another 25 dBi diagonal horn is used on the receiver side at a distance of d = 150 mm. The entire simulation is repeated for the case where the receiver horn is polarized vertically and horizontally. It may seem counter intuitive to have an intentional polarization mismatch between the transmitter and the receiver; however, this results in significant benefits in terms of SNR as we will analyze it further here. The basic circuit components in FPGA are modeled as a 10 mm diameter wire loop placed 0.5 mm above a 50 mm square ground plane encased in a 1 mm thick encapsulant. This model intends to mimic the power connections of the FPGA, so it has a similar size as the FPGA chip. The 3D configuration is shown in Figure 58. The 3 port S-parameter values are simulated using CST's Integral Equation Solver.

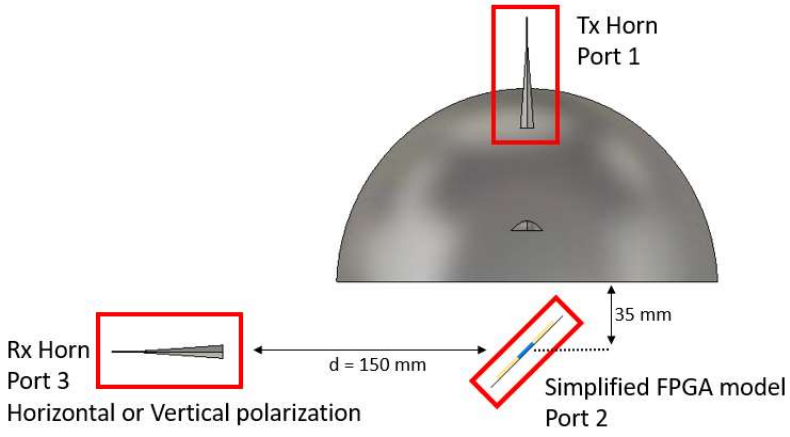


Figure 58 The 3D EM model showing the transmitter, receiver, and the FPGA.

In the next step of the simulation, a switching circuit is inserted into the loop modeled in the 3D EM simulation. The real implementation of the switching circuit that we use in measurements in Section III involves a shift register made of a cascade of

thousands of flip-flops that are all switched at a particular frequency. In the results presented in this section, this frequency is chosen to be 1 GHz and 1.3 GHz and used as the clock of the flip flops. We model the same scenario in ADS at a smaller scale, where we use only a single flip flop as opposed to thousands of cascaded flip flops. Three flip-flops are cascaded and the power lines that supply them are connected to the FPGA loop in the 3D EM model. The flip-flops are realized using NAND gates. A diagram of this configuration is shown in Figure 59.

There are two main paths for the signal from the transmitter to arrive at the receiver. The primary route is simply through specular reflection from the ground plane, mostly explained by S_{31}. This route mostly preserves polarization and involves no nonlinear effects. The secondary route is through modulated scattering from the FPGA circuit. The transmitted signal is initially received by the FPGA circuit, mostly explained by S_{21}. The signal experiences some nonlinear effects due to the active circuit, calculated by the circuit simulation. Finally, the signal is scattered from the FPGA circuit and received by the receiver horn, mostly explained by S_{32}.

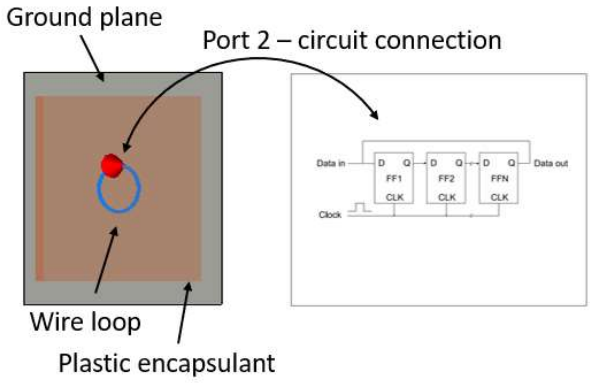


Figure 59 Diagram of the switching circuit that is inserted into the FPGA circuit.

As the excitation signal, we use a 0 dBm 300 GHz carrier with a -90 dBm flat spectrum noise (this value is chosen to be consistent with the noise floor levels of the measured signal in the bandwidth of interest). The simulated received spectrums for the polarization filtered and non-polarization filtered case are shown in Figure 60 Simulated received spectrum when flip-flop shift frequency is (a) 1.0 GHz, (b) 1.3 GHz. The no polarization filtering trace is shifted by 0.05 GHz to prevent overlapping and allow for easier visual comparison.

It should be noted that the frequency peaks exactly overlap in reality, the shift is introduced while plotting to make visual comparison easier. The two traces correspond to two scenarios where the receiver horn (port 3) in Figure 58 is polarized vertically (no polarization filtering) or horizontally (polarization filtering). The case where the horn is polarized horizontally is labeled as "polarization filtering" because it uses deliberate mismatch between the transmitter and the receiver to filter out the undesirable carrier and the noise coming from the transmitter which is predominantly vertically polarized. The 300 GHz carrier, transmitter caused noise, 1 GHz peaks caused by switching activity and its harmonics can be seen for both polarization cases. It can also be seen that the undesirable 300 GHz carrier is approximately 29 dB weaker for the polarization filtered case which is perfectly consistent with the reduction in S_{31} when polarization filtering is used (when Tx is vertical, but Rx is horizontal). This also results in a 29 dB reduction in the transmitter caused noise, which directly translates to an increase in SNR. The desirable 1 GHz modulated peak is slightly stronger for the polarization filtered case. This is due to a slight difference in S_{32} values for the horizontal and vertical receivers. The difference is very much dependent on the geometry of the FPGA model, which was a 10 mm diameter wire

loop and the location at which it is fed. Different geometries such as rectangular and elliptical loops were used to excite different polarization characteristics which resulted in differences in the relative strengths of the modulated peaks, which is to be expected. Only the 10 mm loop result is shown here due to its simplicity.

Since the phenomenon of unintentional modulation depends on a carrier signal injected onto the surface of the FPGA from an outside source, the electromagnetic contribution of every single transistor and connection is relevant. Therefore, an exact simulation of this phenomenon would require every transistor and connection to be simulated in a full wave EM solver. It is infeasible to simulate this level of complexity. Instead, for the proof of concept, we use simplified substitute for the FPGA to mimic the nonlinear effects that cause this unintentional modulation. Moreover, simulating a very low frequency modulation (~1 MHz) onto very high frequency (300 GHz) creates significant difficulties. The duration of the simulation must be long enough to contain dozens of cycles of the low frequency and the time samples must be fine enough to have many samples within a single cycle of the high frequency. For this reason, the modulation frequency is chosen to be 1 GHz in the simulation and 1.6 MHz in measurements shown in Section III.

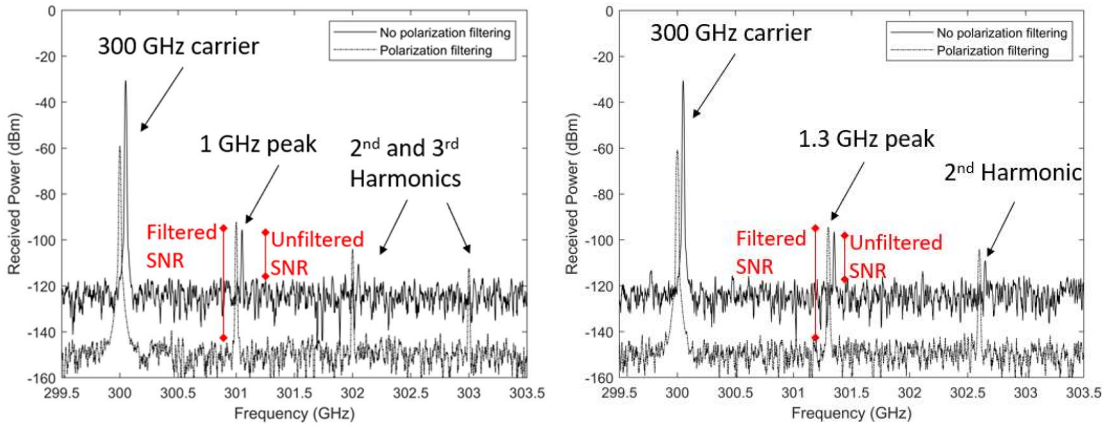


Figure 60 Simulated received spectrum when flip-flop shift frequency is (a) 1.0 GHz, (b) 1.3 GHz. The no polarization filtering trace is shifted by 0.05 GHz to prevent overlapping and allow for easier visual comparison.

6.4 Side Channel Sensing: Polarization and Distance

This section presents the measurement results for the scenario outlined in the previous section. Subsection A describes the details of the equipment, components, and the measurement setup. Subsection B presents the measured SNR values obtained from a 2D scan of the FPGA and the difference that polarization makes at a fixed receiver to FPGA distance. Finally, Subsection C describes effect of receiver to FGPA distance has on the SNR.

6.4.1 Measurement Setup

The concept of backscatter side channels as described in Section II is realized at 300 GHz using a Terasic board with Altera Cyclone V FPGA, custom made Virginia Diodes 300 GHz transmitter (Tx-271) and receiver (Rx-159) pair, optical positioning tools to ensure alignment and proper scanning. The transmitter is connected to a 25 dBi diagonal horn antenna [58] which feeds the 20 cm diameter elliptical near field focuser with a 0.7

mm 3 dB spot size that is 35 mm away from the aperture of the main reflector as detailed previously. The model shown in Figure 56 was fabricated. The main reflector is carved out of an aluminum block using a CNC lathe, the subreflector and the struts holding it are 3D-printed. The fabricated prototype is shown in Figure 61 (a). The focuser illuminates a 0.7 mm diameter spot on an FPGA that angled at 45 degrees and is mounted on two Zaber brand micron precision positioners which move it vertically and at a 45° angle [59].

Figure 61 (a) The fabricated prototype of the model ellipsoidal. (b) 300 GHz backscatter side channel measurement setup.

The FPGA is toggling its gates at a frequency of 1.6 MHz to create the unintentional modulation. The backscattered signal is received by the receiver that is connected to an identical diagonal horn antenna. The receiver is d = 150 mm away from the board unless stated otherwise. All of the components are fixed to an optical breadboard and optical rails for alignment. The measurement setup is shown in Figure 61 (b).

There is a high variability of signal strength and noise floor based on which region of the FPGA is illuminated by the transmitter. Two hot spots were identified on the FPGA board by a 2D scan with a resolution of 1mm: a capacitor region on the board and the center

of the FPGA chip. Two 6 mm by 7 mm region that contain these hotspots were further scanned with more precise 0.5 mm increments to get a better understanding of the signal variation and find the optimum spot for best signal. Cell dimension corresponds to the spot size of ellipsoidal transmitter used in measurements. These rectangular regions are highlighted in Figure 62.

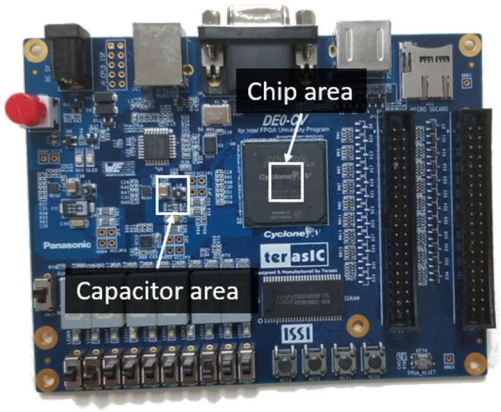


Figure 62 The rectangular regions that contain the hotspots.

6.4.2 Effect of Polarization Filtering

In this EM backscattering side channel measurement scheme, we are only interested in the signals that are modulated onto the carrier frequency. The reception of the carrier signal itself and all other artifacts created by the transmitter are an undesirable consequence of the method. Also, since the entire mechanism uses the FPGA as an unintentional modulator, the desired signal ends up being much weaker (e.g. 40 dB) than the carrier. This relatively much stronger carrier signal causes significant saturation problems in the receiver due to issues with dynamic range. Using a millimeter wave filter is infeasible since the modulation frequency is very small compared to the carrier (~2 MHz vs. 300 GHz), the filter would require an infeasibly sharp response to reject the undesired 300 GHz carrier

without reducing the modulated signal. Moreover, the imperfections of the transmitter create a noise floor higher than that of the thermal noise floor of the receiver.

The transmitter is configured to create a vertically polarized spot on the FPGA. Most of the transmitted wave, containing a strong carrier and transmitter noise, is specularly reflected from the surface and remain vertically polarized. A small part of the incident wave is absorbed, unintentionally modulated, and backscattered. This backscattered component is what we are interested in and its polarization depends on the bondwires, traces, connection routing, etc. in the FPGA. This makes the polarization difficult to predict exactly; however, we know that it is not necessarily vertical.

To reduce the effect of the carrier and the transmitter noise, we introduce a polarization mismatch between the transmitter and the receiver as shown in Figure 63. The receiver is converted from vertical to horizontal polarization using a 90 degree waveguide twist from Virginia Diodes [60]. This filters out a significant portion of the specularly reflected carrier and transmitter noise which is almost entirely vertically polarized.

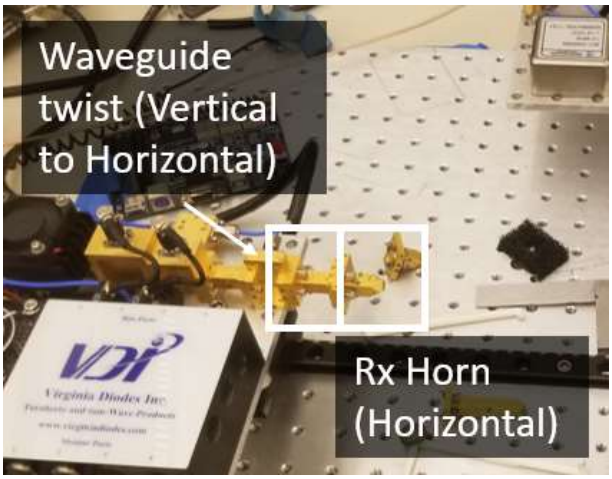


Figure 63 The measurement setup using polarization filtering.

Comparison of measured spectrums with and without polarization filtering is shown in Figure 64. The 300 GHz carrier is suppressed by 20 dB (-28 dBm vs -48 dBm), this helps prevent receiver saturation and shows that the carrier is almost entirely vertically polarized. The noise floor around the frequency of interest is reduced by 11 dB (-122 dBm vs. -133 dBm), this is because the noise floor is elevated due to the transmitter nonidealities. Finally, most interestingly, the signal of interest is enhanced by 2 dB (-77 dBm vs -75 dBm). As stated earlier, the backscattered signal of interest is not necessarily vertically polarized, in fact it has a greater horizontal component than vertical component. Indeed, a similar enhancement of 2 dB was also observed in simulation for the simplified FPGA model consisting of a circular wire loop. The combined effect of an 11 dB reduction in noise floor reduction and 2 dB signal power enhancement yields a 13 dB increase in SNR.

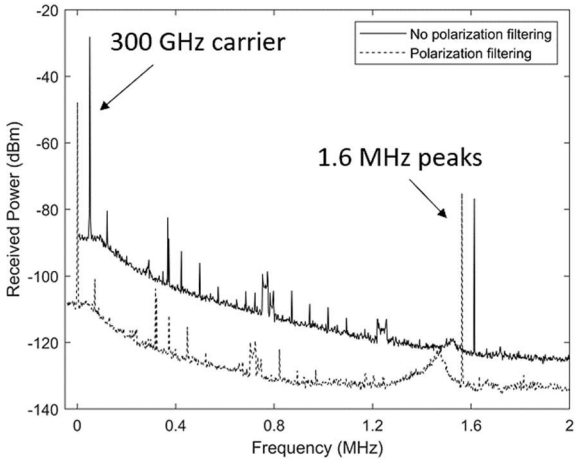
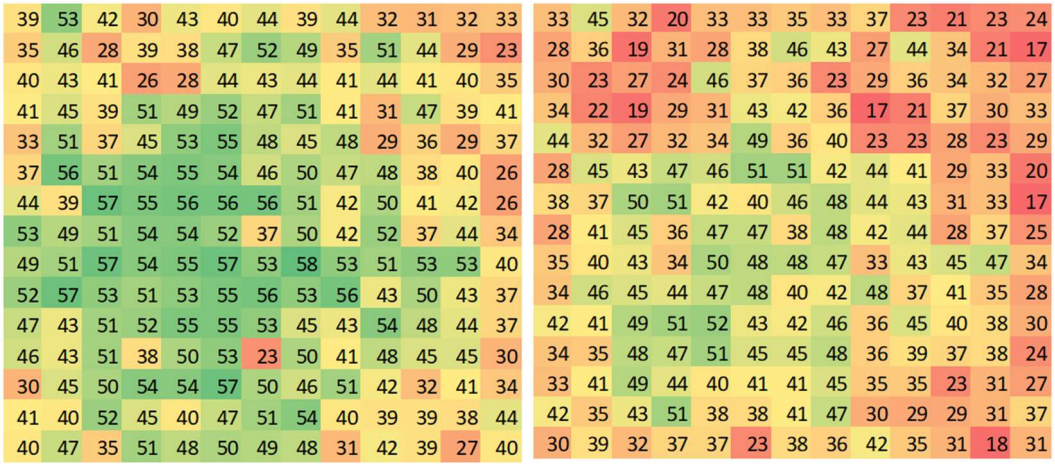


Figure 64 Spectrums measured from the capacitor area with and without polarization filtering. The no polarization filtering trace is shifted by 0.05 MHz to prevent overlapping and allow for easier visual comparison.

This measurement was conducted for the two 6 mm by 7 mm regions that are highlighted as capacitor area and chip area in Figure 62. The entire region was scanned with 0.5 mm increments resulting in 13 by 15 data points.

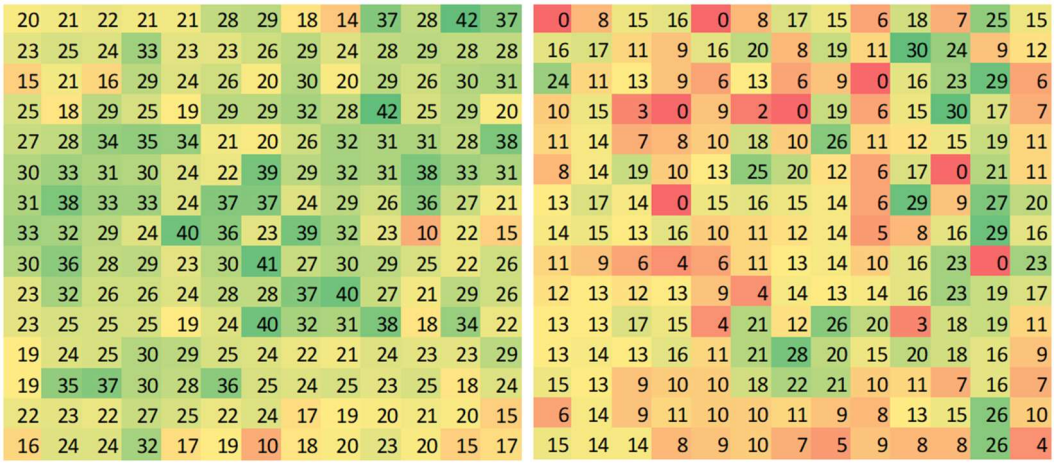
The SNR values measured from the capacitor area are shown in Figure 65. In Figure 65 (a) the SNR values with the polarization filtering can be seen. The highest values are localized in a roughly circular region corresponding to the location of the capacitor. An average SNR value of 48 dB with a maximum of 58 dB is observed. In Figure 65 (b) the SNR values without the polarization filtering can be seen. Similar to the filtered case, the highest values are localized in a roughly circular region corresponding to the location of the capacitor. An average SNR value of 36 dB with a maximum of 52 dB is observed. It can be seen that polarization filtering yields 12 dB better SNR on the average. This is due to a 2 dB signal strength increase on the average and 10 dB noise floor reduction on the average. The noise floor values measured from each spatial sample showed significant variation for both cases (-130 dBm to -150 dBm with polarization filtering, -120 dBm to -140 dBm without polarization filtering). The highest SNR values were measured close to the center of the capacitor region for both filtered and unfiltered cases.

Similar SNR results were obtained from the chip area as shown in Figure 66. The signal levels are approximately 20 dB weaker for the chip area as compared to the capacitor area. This could be due to the interference of the plastic encapsulant material that protect the FPGA and the interconnections. The highest SNR values for the filtered case is located close to the center whereas for the unfiltered case the highest SNR values were measured towards the top right corner of the highlighted region. Average SNR is enhanced by 15 dB. For this region, polarization filtering is significantly more impactful. Most importantly, there are weak spots for the unfiltered case where little to no signal is received (0 dB SNR) whereas the enhancement from polarization filtering was enough to boost the SNR to a level that can be detected anywhere.



(a) (b)

Figure 65 Measured SNR values in dB from the capacitor area: (a) with polarization filtering (average 48 dB) and (b) without polarization filtering (average 36 dB). (0.5mm resolution)



(a) (b)

Figure 66 Measured SNR values in dB from the chip area in dB: (a) with polarization filtering (average 27 dB) and (b) without polarization filtering (average 12 dB).

6.4.3 Effect of distance

There is significant difference when it comes to the noise characteristics of the signal with and without polarization filtering. The primary source of the noise is not the thermal noise of the receiver but instead the unintentionally generated signals coming from the transmitter and the FPGA. This means the SNR will decay slower than $1/r^2$.

The change in measured SNR for receiver distances of up to 45 cm is shown in Figure 67 for both with and without polarization filtering. The polarization filtered case has better SNR for all distances. The decay trend is indeed slower than $1/r^2$ as predicted. For even longer distances, the noise created by the transmitter would start to be dominated by the thermal noise of the receiver and the SNR behavior would start to follow a $1/r^2$ trend. The measurements were only taken up to 45 cm due to the limitations caused by the length of the optical flat plane on which the equipment was placed. The SNR values measured at this 45 cm limit are 44 and 54 dB for unfiltered and filtered configurations respectively, indicating that the signal can be detected at distances much farther than 45 cm.

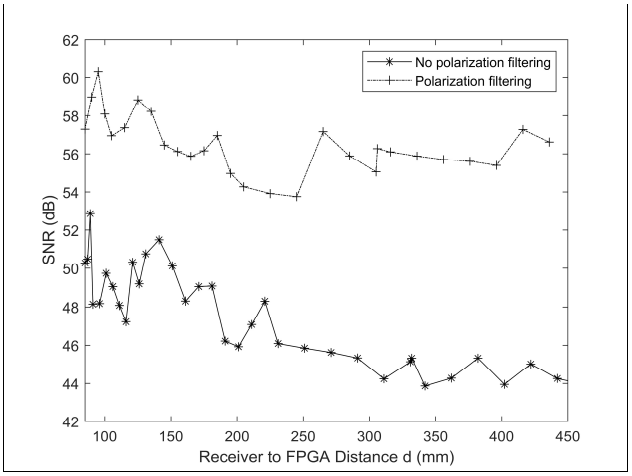


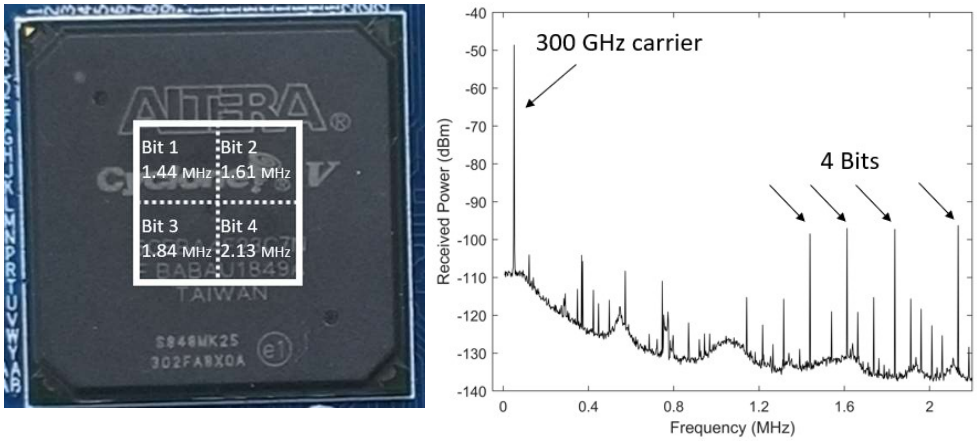
Figure 67 The SNR behavior as the distance between the receiver and FPGA increases with and without polarization filtering.

6.5 Side Channel Sensing: Multiple bits

In previous sections, the FPGA was configured to switch all of its gates at the same frequency. This allows for maximum signal strength for a single modulated peak, in other words a 1-bit backscattered side channel. However, thanks to the additional SNR that can

be achieved with polarization filtering, it is possible to excite and detect such unintended backscattered peaks at multiple frequencies (bits) simultaneously. Increase in the number of bits that can be backscattered in parallel increases the capacity of how much data can be detected, which has great benefits for practical side channel applications such as monitoring the behavior of an IC, secretly transmitting data using malicious hardware modifications such as Hardware Trojans, or deliberately toggling FPGA gates to create an antenna-less RF transceiver using nothing but an FPGA which can be used as RFID device.

In this section we divide the FPGA into 4 modules and switch the gates in each module at a different frequency. This creates a 4-bit channel where each bit corresponds to a different physical location on the chip as shown in Figure 68 (a). The measurement set up used is shown in Figure 61 (b) with a distance d = 15 cm. The overall signal received from the chip is shown in Figure 68 (b).



(a) (b)

Figure 68 (a) Location and the frequencies of modules that create the 4 bits. (b) Spectrum received from the entire chip.

Moreover, the usage of a THz focuser allows for the spatial analysis of this side channel phenomenon. In a practical application, the FPGA will not be configured such that

the entire chip does a single task. It will have different modules in different locations with different tasks and different electromagnetic signatures. It is desirable for a focused measurement scheme to be able to amplify the signal of one module while keeping the interference from other modules to a minimum. With the 4-bit FPGA configuration, we try to measure how much the signal from a single module can be isolated from other modules. Since a smaller part of the FPGA is generating each bit, the signal strength is lower compared to the 1-bit configuration. For this reason, the measurements are only done using the polarization filtering technique.

To quantify how much the signal of a single module (in other words a single bit) can be emphasized over others, we find the spatial locations where that bit is the strongest and compare its signal strength with the signal strength of the second strongest bit (a positive value). To quantify how much the signal of a single bit can be filtered out, we find the spatial locations where that bit is not the strongest and compare its signal strength with the signal strength of the strongest bit (a negative value).

The spectrums received from the most dominant and least dominant locations for bit 1 is shown in Figure 69. For the spectrum where Bit 1 is the most dominant, it is 6.8 dB stronger than the second strongest bit received from that location. This means, if we were only interested in the signals coming from Bit 1 region, we could target the focuser on this location and reduce the interference from other modules by at least 6.8 dB. For the spectrum where Bit 1 is the least dominant, it is 11.3 dB weaker than the strongest bit received from that location. This means, if Module 1 was creating significant interference that we didn't want to receive, we could target the focuser on this location and maximally limit the contribution of Module 1 compared to other modules.

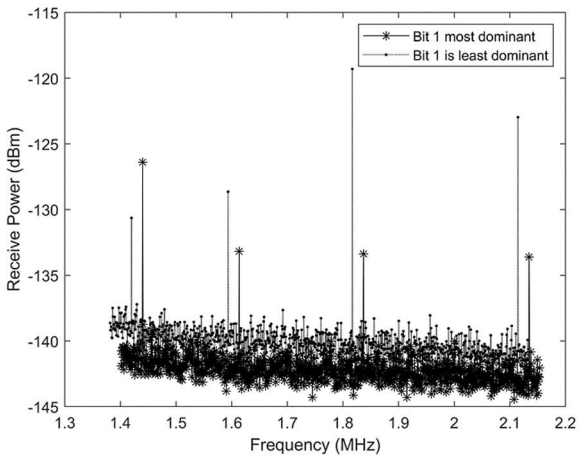


Figure 69 The spectrums received from the spatial samples that yielded the most dominant and the least dominant results for Bit 1.

The analysis described above has been done for the entire chip area and the results are shown in Figure 70. The two optimum locations that yield -11.3 dB and 6.8 dB can be found here. The most important thing to note here is the lack of any apparent order. Intuitively one might expect that the signal coming from Bit 1 would be the most dominant when the focuser targets the location that corresponds to Module 1. In a practical side channel application it would be convenient if this were the case. With only the knowledge of the locations of the modules, a focuser could be directed at the optimal spot without any guess work or any need for scan. Unfortunately, this is not what we observe. The locations where a module is dominant or not seems to be scattered randomly. This reinforces the idea that this modulation is not created primarily by the logic circuit itself but instead the supplementary circuits around it such as bondwires, connection blocks, power connections, capacitor connections, etc. This is not true, transistor is created by logic circuits, but signal is weak and leaks the strongest at bondwires, capacitors, etc. The location of a module on an FPGA is easier to control compared to these supplementary circuits which could explain

the lack of correlation between the location where certain modules are most and least dominant.

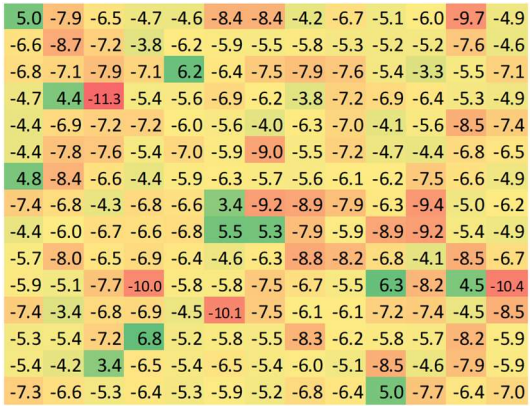


Figure 70 The spectrums received from the spatial samples that yielded the most dominant and the least dominant results for Bit 1.

This analysis is done for all 4 bits. The most dominant and least dominant signal values for each bit is shown in Table . Other than Bit 4 having slightly greater variance, there is no significant difference between the level of dominance between bits. To reemphasize, the values quoted in this section are not SNR values, they are variances in the SNR between the bits and how much they are greater or lower than the SNR of other bits.

Table 4 Best achieved relative strengths that emphasize or filter out a single bit/module.

	Most Dominant (w.r.t. second most dominant bit)	**Least Dominant (w.r.t. most dominant bit)**
Bit 1	6.8 dB	-11.3 dB
Bit 2	6.7 dB	-9.5 dB
Bit 3	6.4 dB	-10.7 dB
Bit 4	7.3 dB	-11.9 dB

As mentioned previously, there is no apparent correlation between the locations of the modules and optimal signal locations. However, this lack of correlation does not mean

the ability to focus on different spatial locations is not useful. As we show in Table , for any particular bit, it is possible to find a spot where it is at least 6.4 dB stronger than all the other bits and a spot where it is at least 9.5 dB weaker than all the other bits. All the benefits of being able to focus on a single module over other modules is still realizable as long as these optimal locations are characterized by a 2D scan of the FPGA.

6.6 Sensing side channels at long ranges via a receiver

In practical applications such as RFID and hardware Trojan detection, it is desirable to be able to detect these signals at longer ranges while maintaining high SNR. For this purpose, we use a reflector antenna on the receiver side in addition to the near field focuser on the transmitter side. We also explore the effects of positioning the receiver at various angles pointed at the FPGA.

6.6.1 Sensor geometry, fabrication, and measurement

This section presents THz receiving reflector design for side channels detection and range extension. The geometry of the reflector system is shown in Figure 71 and the parameters are shown in Table . The diameter of the reflector was chosen to be 191 mm due to the constraints on the physical dimensions imposed by the measurement system and optical equipment available. The feed is chosen as the 25 dBi diagonal horn which is a part of the THz measurement system. The rest of the reflector design methodology is the same as in Chapter 5. Similarly, we use the concept of shifting the secondary reflector axially to change the location of the focus, L_{focus}. To deliberately shift the secondary reflector axially, we use four sets of struts with different lengths. This results in $L_{secondary}$ values of 91 mm, 93 mm, 95 mm, 97 mm and associated L_{focus} values of 0.95 m, 1.13 m, 1.37 m, 1.78 m. All

four of these reflector configurations are designed to have 52 dBi near field directivity, providing a 6 dBi improvement over the reflector used in Chapter 5. This is consistent with the quadrupling of the surface area of the reflector.

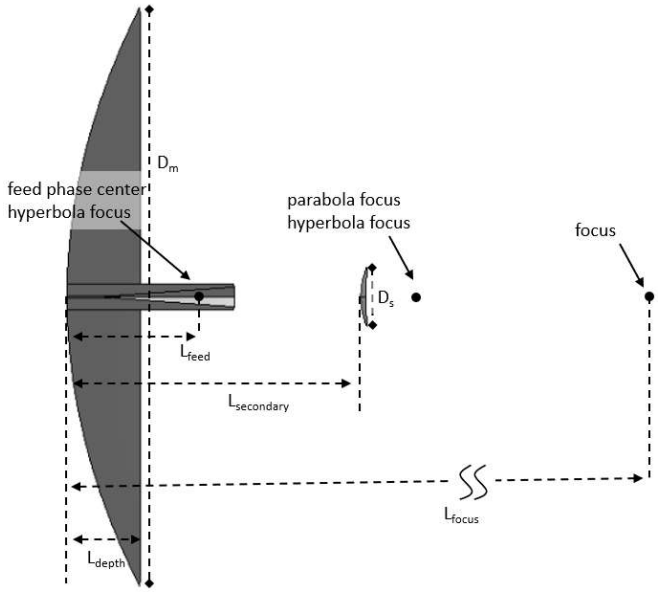
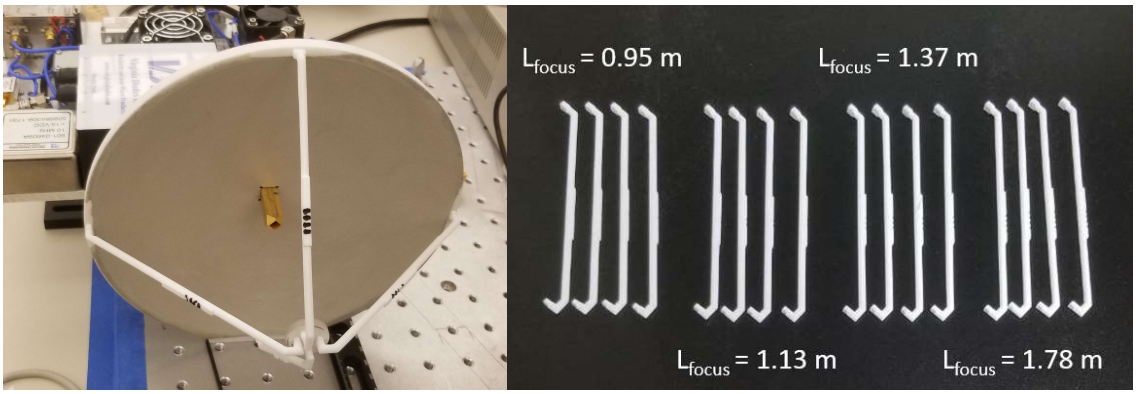


Figure 71 Long distance focuser geometry.

Table 5 Design parameters for the paraboloid long range reflector

$\boldsymbol{D_m}$	191 mm	Primary reflector diameter
$\boldsymbol{f_m}$	95 mm	Primary reflector focal length
$\boldsymbol{D_s}$	19.4 mm	Secondary reflector diameter
$\boldsymbol{a_s}$	14 mm	Secondary reflector hyperbola parameter
$\boldsymbol{b_s}$	18.3 mm	Secondary reflector hyperbola parameter
$\boldsymbol{L_{feed}}$	48.9 mm	Feed point offset w.r.t. primary reflector vertex
$\boldsymbol{L_{secondary}}$	91 mm, 93 mm, 95 mm, 97 mm	Distance between the vertices of the main and the secondary reflectors
$\boldsymbol{L_{focus}}$	0.95 m, 1.13 m, 1.37 m, 1.78 m	Distance between the focus spot and the vertex of the primary reflector

The prototype for the receiver reflector is manufactured out of 3D printed nylon using EOS Formiga P110 printer that uses selective laser sintering method. Due to the way 3D printing works, this results in a product with some surface roughness which needs to be smoothed using sandpaper. Finally, to make the surface reflective, silver paint is applied and smoothed again. This procedure is explained in detail in section 5.2.4. A picture of the fabricated prototype is shown in Figure 72 (a). In the picture it is using the struts designed to create a focus at 0.95 m. Pictures of the replaceable struts are given in Figure 72 (b).



(a) (b)

Figure 72 (a) Fabricated prototype of the long range receiver reflector. (b) Fabricated struts.

Next, we characterize the performance of the reflector itself. The relevant performance figures are focus depth, focus width, and near field directivity. To do this, we measure the transmission coefficient between the reflector antenna and the open ended waveguide and compare that with the simulation results. However, there are significant challenges due to extreme sensitivity to alignment caused by very high directivity. A flat surface is required, however the optical ground plane on which the components have been previously mounted is not large enough for this measurement. For this reason, the experiments are done on the floor, which was the flattest surface available that was large

enough. Moreover, to ensure alignment, the setup needed to be hand tune for every data point. The tuning process is time consuming which has resulted in fewer data points than desired. The measurement setup can be seen in Figure 73. In this particular picture, 5 pieces of A4 paper is placed beneath the reflector as shims to ensure alignment.

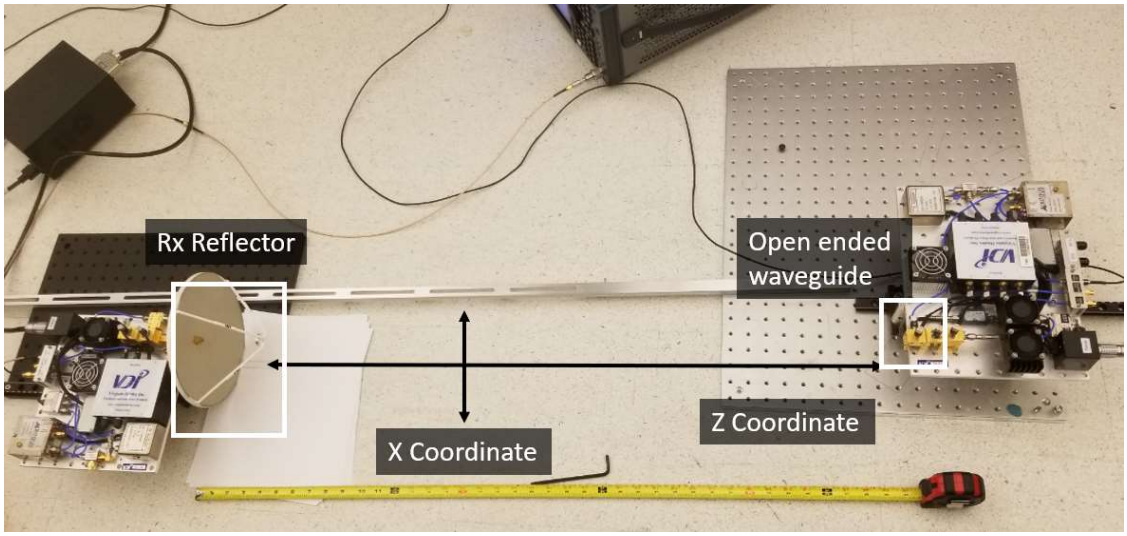


Figure 73 Reflector performance measurement setup.

The measured relative power density values are given in Figure 74. Good agreement is observed in the focus depth values with a slightly shorter focus distance. This is possibly due to the struts not going in fully into the designed holes, causing the subreflector to be slightly farther away from the feed, causing the focus to shift closer. The measured loss was 1.2 dB. This is higher compared to Chapter 5. This could be explained by the added difficulty of aligning the larger reflector at a farther distance. In addition to this, the orientation of the main reflector was upright in the 3D printer as opposed to lying flat, which is suboptimal in terms of surface quality. That also could have factored into the extra 0.5 dB loss.

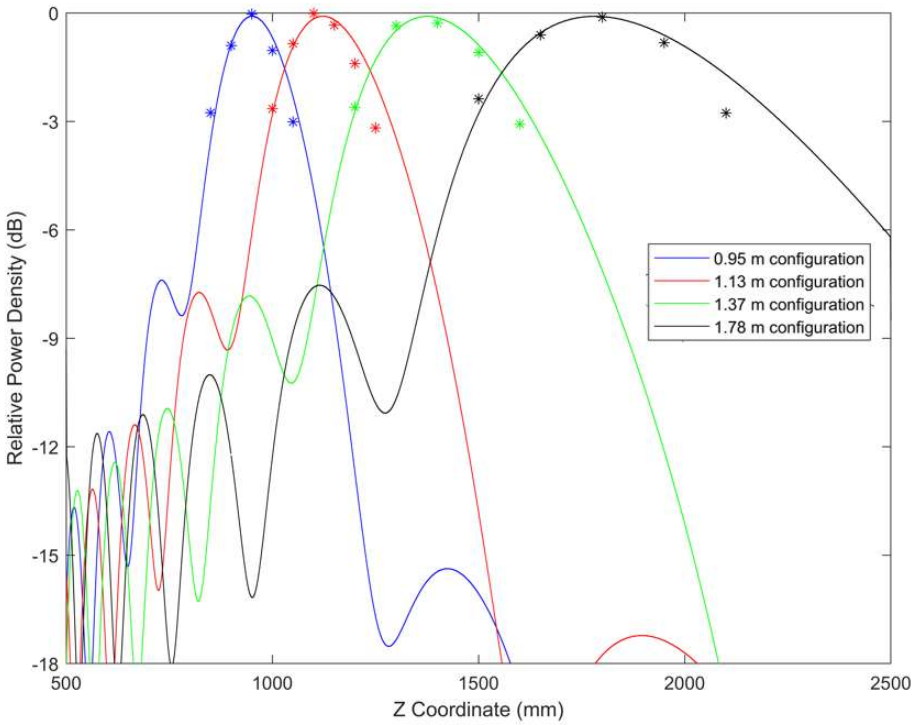


Figure 74 Simulated vs Measured power densities for different strut length configurations.

6.6.2 Measured side channels

With the reflector itself characterized, we then use it to measure backscattered side channels at farther distances. The part of the measurement setup concerning the transmitter and the FPGA is the same, whereas the receiver is placed significantly farther away. This measurement setup can be seen in Figure 75.

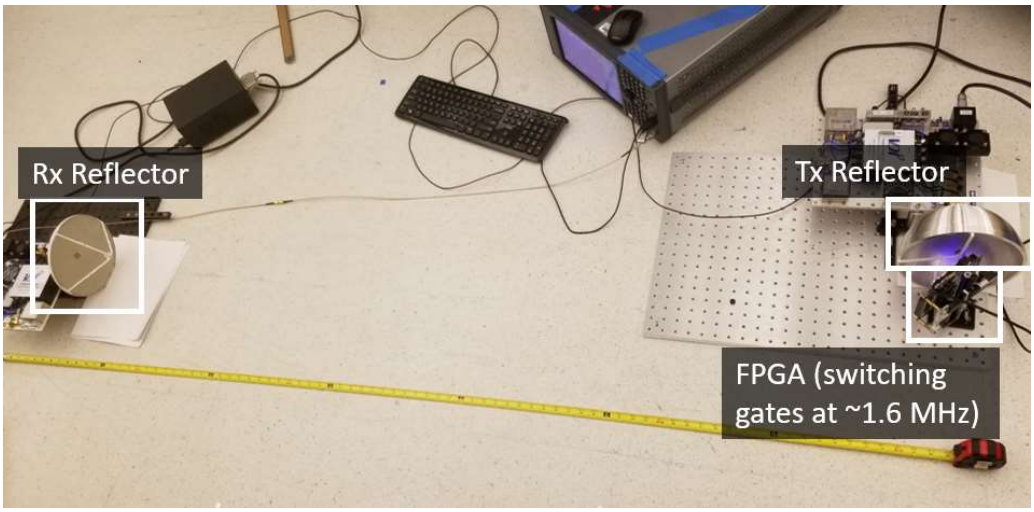


Figure 75 Backscattered side channel measurement setup at 1.78 m.

Since the main purpose of this reflector is to enable greater ranges of detection, the spectrum for the maximum distance configuration of z = 1.78 m is provided in Figure 76. There are several things worth noting. The transmitter is focused on the chip area as opposed to the capacitor area, which is the more challenging of the two scenarios. In section 6.4.2, it is shown that the chip area has lower SNR values than the capacitor area. However, the chip area has been selected as the testing region due to it providing an opportunity to preferentially target different modules for future applications. The measured SNR for the side channel signal in this configuration is 39 dB. Polarization filtering has not been used. The noise floor of the received spectrum is flat, meaning it is no longer caused by the transmitter.

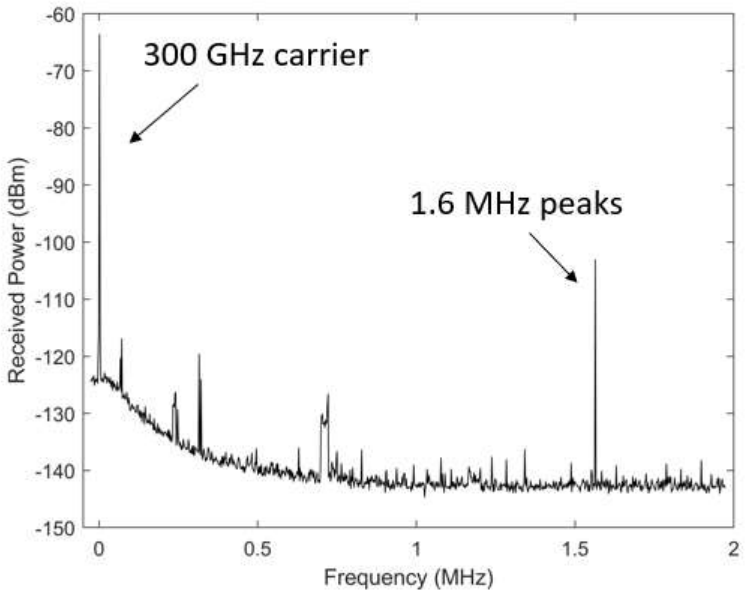


Figure 76 Received spectrum of the backscattered side channel at a distance of 1.78 m.

6.7 Conclusions

We present a backscattered side channel sensing scheme at 300 GHz using an ordinary FPGA not designed to operate anywhere close to this band. A proof of concept EM-circuit co-simulation analysis of this surprising phenomenon is given using a structurally simplified FPGA model and a near field focuser. In these simulations, the effect of polarization is also explored. Specifically, creating a deliberate polarization mismatch between the receiver and the transmitter. This is shown to suppress the very strong undesirable carrier signal significantly and reducing the high level of noise created by the transmitter. We realize this 300 GHz backscattered side channel using an ordinary FPGA that is configured to flip its gates at a particular frequency single frequency transmitting a single bit. This backscattered side channel was measured to have an SNR as high as 36 dB, which was further elevated to 48 dB using the proposed polarization filtering technique. In addition to this, we use a 300 GHz near field focuser to scan the FPGA with a resolution

of 0.7 mm to find hotspots for these backscattered signals and characterize spatial variance. Furthermore, the FPGA is then configured to have 4 different modules flipping its gates at 4 different frequencies thereby transmitting 4 bits in parallel, which greatly improves the capacity for practical side channel applications. Furthermore, the spatial resolution and the scanning capability of the near field focuser is used to scan the FPGA to find spatial variances between these 4 modules, with the purpose of isolating to enhance or reject the signal from each module. It was found that it is possible to find distinct spots where each of the modules can be enhanced to be at least 6.4 dB stronger than the other modules. Finally, a 20 cm paraboloid reflector is designed, manufactured, and tested to show that these measurements can be done at 1.8 m away with 40 dB SNR.

CHAPTER 7. RESEARCH CONTRIBUTIONS AND FUTURE WORK

7.1 Research Contributions

This research detailed the design and analysis of EM sensors and measurement schemes for EM side channel detection as well as developing a deeper insight into the fundamental mechanisms that give rise to backscattered side channels. The low signal levels and the unusual mechanisms by which they are generated, makes it necessary for side channel detection to use sensors that are specifically designed for this purpose. The sensor designs and measurement schemes provided in this thesis allow for much more effective side channel techniques. The research contributions of this thesis are:

1. We propose a novel high gain planar antenna array for side channel detection at 1 GHz. The design of the antenna is optimized to provide high gain while being extremely inexpensive and simple manufacture. This is achieved primarily by using slotted circular disc elements that operate in a higher order TM_{12} mode, which allows each element to be 6 dB more directive than an ordinary patch antenna. Then a 2x2 array of these elements are fed by electromagnetically coupling an identical element between the array and the ground plane. The elements are made out of sheet metal which can be manufactured inexpensively and suspended over a ground plane using plastic screws, making it unnecessary to use any circuit printing technique while at the same time avoid all dielectric losses. The achieved gain is 19 dBi with a bandwidth of 6.7%. We then use this antenna to measure side channels from an IoT device at distances ranging from 1-5 meters and characterize the effect of noise [61].

2. We present a novel near field backscattered side channel measurement scheme and a sensor topology that consists of a combination of E and H field probes that excite a carrier signal on an FPGA and detect the signal that is unintentionally modulated onto this carrier by the FPGA at 3 GHz. This application is determined to have a requirement of 1 mm resolution and better than 20 dB mutual coupling between the probes, which is successfully achieved. A proof of concept EM-circuit simulation of the surprising unintentional FPGA backscattering phenomenon is provided to develop deeper insight into this mechanism. It is shown that the backscattered signal carries a signature of the underlying circuit, which has great potential in detecting Hardware Trojans. Indeed, the proposed probe combination and the measurement scheme is used to detect Hardware Trojans injected into realistic FPGA configurations with an accuracy of 100% for a sample size of 40 [62].
3. We present a THz backscattered side channel measurement scheme and a THz near field focuser reflector. The reflector is designed for 300 GHz, is fed by a 25 dBi metallic diagonal horn antenna, has a diameter of 10 cm, focused nearfield directivity of 46 dBi, focus width and depth of 4 mm and 10 cm respectively. The reflector is manufactured using 3D printing and metalized using silver paint. The nonidealities such as surface roughness, conductivity, layer thickness of such techniques, especially at a frequency as high as 300 GHz needed to be characterized. Upon theoretical analysis and measurements, we verified that the outlined manufacturing technique was sufficient to achieve less than 1 dB loss for a reflector based antenna. This antenna is then used in the described backscattered

side channel measurement scheme to extend the detection range to beyond 5 cm, up to 28 cm [63].

4. We examine the effect of polarization on THz backscattered side channels. We identify a major bottleneck in THz backscattered side channels to be the noise that is created by the transmitter that is used to excite a very strong 300 GHz carrier signal in an FPGA. This noise coming from the transmitter is found to be significantly higher than the thermal noise floor of the receiver, unnecessarily degrading the SNR. Several approaches to solving this issue is examined. A proof of concept EM-circuit simulation is developed to gain some insight into the mechanism of this type of side channel. In simulation, it is shown that introducing an intentional mismatch between the transmitter and the receiver significantly reduces the noise coming from the transmitter while having minimal effect on the desired backscattered signal. These findings are then replicated in measurements to provide 12 dB increase in SNR [64].

   Additionally, we purpose a 20 cm diameter ellipsoidal reflector that is capable of creating a 0.7 mm focus. We use this to scan the surface of the FPGA with 0.5 mm resolution to identify hotspots where the backscattered signal is the strongest, the capacitor area and the chip area. We then leverage the spatial resolution of the measurement setup to distinguish the signals coming from different modules in an FPGA. For this setup, we split the FPGA are into 4 modules where each module is creating a side channel at a different frequency. In practical side channel techniques, it would be very desirable to be able to focus on the signal coming from

just a single one of these modules. We show that it is possible to preferentially receive the signal coming a single module with a clearance of 6 dB.

Finally, we design and use a 20 cm diameter paraboloidal reflector as a receiver to extend the range of these techniques to beyond a meter. We show that SNR values of around 40 dB can be received at 1.8 meters from the chip area which is the more challenging scenario.

7.2 Future Research Directions Work

Although we have been able to create proof of concept simulations showing the viability of backscattered side channels, these simulations are not accurate enough to have predictive power regarding more nuanced properties of the side channel signals. As explained, an accurate simulation would require the entire IC to be modeled in a 3D EM simulation because the backscattering setup interacts with the entirety of the chip electromagnetically, having the whole chip in a circuit simulation would be of no use. Unfortunately, having the entire chip in a 3D EM simulation in a straightforward way is not anywhere close to being feasible. However, a middle ground could be possible. One approach would be to separate a chip into small rectangular segments and have the interconnects modeled in 3D EM simulation and each segment would be modeled as a circuit. The segments could be modeled as finely as the spatial resolution of the measurement scheme requires, such as 1 mm^2 or 0.25 mm^2 etc.

We have used the concept of polarization filtering to great effect in practical THz backscattered side channel detection, however we did not do a very detailed analysis of the kind of polarization coming off of the FPGA, such as precise description of the polarization

such as diagonal or elliptical polarization etc. This is primarily due to the limitations of the equipment. The receiver we use to detect 300 GHz signals loses phase information. Moreover, it is very bulky and sensitive at the same time, so physically rotating while preserving the strict requirements on alignment is difficult. With a more complex setup, precise polarization can be measured.

Finally, although we were able to identify spatial variations over the FPGA in the THz backscattered side channel measurement setup, we did not go into the details of these variations. Moreover, the 2D scan of the FPGA was limited by the resolution of the 20 cm diameter ellipsoidal reflector with a spot size of 0.7 mm. With a higher resolution reflector and a high resolution scanning setup (which might go into higher frequencies than 300 GHz to make a smaller focus spot easier to achieve), much more detailed results can be achieved. With a higher resolution setup, every individual bond wire, every module could be separately targeted.

REFERENCES

[1] C. Cheng, L. N. Nguyen, M. Prvulovic and A. Zajić, "Exploiting Switching of Transistors in Digital Electronics for RFID Tag Design," in *IEEE Journal of Radio Frequency Identification*, vol. 3, no. 2, pp. 67-76, June 2019.

[2] R. Callan, A. Zajic, M. Prvulovic, "A Practical Methodology for Measuring the Side-Channel Signal Available to the Attacker for Instruction-Level Events", *Microarchitecture (MICRO) 2014* , pp. 242-254, 2014.

[3] D. Agrawal, B. Archambeult et al., "The EM side-channel(s)," in *Proc. Crypto. HW and Emb. Sys. (CHES)*, 2002, pp. 29–45.

[4] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis: leaking secrets," in *Proceedings of CRYPTO'99*, Springer, Lecture notes in CS, 1999, pp. 388–397.

[5] A. Nazari, N. Sehatbakhsh, M. Alam, A. Zajic, and M. Prvulovic, "Eddie: Em-based detection of deviations in program execution," in *Proceedings of the 44th Annual International Symposium on Computer Architecture*, 2017, pp. 333–346.

[6] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi and B. Sunar, "Trojan Detection using IC Fingerprinting," *2007 IEEE Symposium on Security and Privacy (SP '07)*, Berkeley, CA, 2007, pp. 296-310.

[7] C. He, B. Hou, L. Wang, Y. En and S. Xie, "A failure physics model for hardware Trojan detection based on frequency spectrum analysis," *2015 IEEE International Reliability Physics Symposium*, Monterey, CA, 2015, pp. PR.1.1-PR.1.4.

[8] N. Sehatbakhsh, A. Nazari, A. Zajic, and M. Prvulovic, "Spectral profiling: Observer-effect-free profiling by monitoring em emanations," in *Microarchitecture, 2016 49th Annual IEEE/ACM International Symposium on*. IEEE, 2016, pp. 1–11.

[9] J. Villasenor, "The hacker in your hardware," *Sci. Amer.*, no. 2, pp. 82–87, 2010.

[10] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware trojan: Threats and emerging solutions," in *Proc. IEEE Int. High Level Design Validation Test Workshop*, Nov. 2009, pp. 166–171.

[11] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design Test Comput*., vol. 27, no. 1, pp. 10–25, Jan. 2010.

[12] L. N. Nguyen, C. Cheng, M. Prvulovic and A. Zajić, "Creating a Backscattering Side Channel to Enable Detection of Dormant Hardware Trojans," in *IEEE Transactions on VLSI Systems*, vol. 27, no. 7, pp. 1561-1574, July 2019.

[13] D. Uchida, T. Nagai, Y. Oshima and S. Wakana, "Novel high-spatial resolution probe for electric near-field measurement," *2011 IEEE Radio and Wireless Symposium*, Phoenix, AZ, 2011, pp. 299-302.

[14] Yingjie Gao and I. Wolff, "Miniature electric near-field probes for measuring 3-D fields in planar microwave circuits," in *IEEE Transactions on Microwave Theory and Techniques*, vol. 46, no. 7, pp. 907-913, July 1998.

[15] G. Li, K. Itou, Y. Katou, N. Mukai, D. Pommerenke and J. Fan, "A Resonant E-Field Probe for RFI Measurements," in *IEEE Transactions on Electromagnetic Compatibility*, vol. 56, no. 6, pp. 1719-1722, Dec. 2014.

[16] Y. Park, J. Bang, K. Jung, et al., "Design of a Broadband Electric Near-Field Probe With Improved Sensitivity Using Additional Tips," *2018 International Symposium on Antennas and Propagation (ISAP)*, Busan, Korea (South), 2018, pp. 1-2.

[17] I. F. Akyildiz, C. Han and S. Nie, "Combating the Distance Problem in the Millimeter Wave and Terahertz Frequency Bands," in *IEEE Communications Magazine,* vol. 56, no. 6, pp. 102-108, June 2018.

[18] Y. J. Cheng and F. Xue, "Ka-Band Near-Field-Focused Array Antenna with Variable Focal Point," in *IEEE Transactions on Antennas and Propagation*, vol. 64, no. 5, pp. 1725-1732, May 2016.

[19] H. D. Hristov and M. H. A. J. Herben, "Millimeter-wave Fresnel-zone plate lens and antenna," in *IEEE Transactions on Microwave Theory and Techniques*, vol. 43, no. 12, pp. 2779-2785, Dec 1995.

[20] S. Karimkashi, A. A. Kishk, "Focusing properties of Fresnel zone plate lens antennas in the near-field region", *IEEE Trans. Antennas Propag*., vol. 59, no. 5, pp. 1481-1487, May 2011.

[21] P. F. Li, S. W. Qu, S. Yang and Z. P. Nie, "Microstrip Array Antenna With 2-D Steerable Focus in Near-Field Region," in *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 9, pp. 4607-4617, Sept. 2017.

[22] L. Shan and W. Geyi, "Optimal Design of Focused Antenna Arrays," in *IEEE Transactions on Antennas and Propagation*, no. 11, pp. 5565-5571, Nov. 2014.

[23] H. T. Chou, T. M. Hung, N. N. Wang, et al., "Design of a Near-Field Focused Reflectarray Antenna for 2.4 GHz RFID Reader Applications," in *IEEE Transactions on Antennas and Propagation*, vol. 59, no. 3, pp. 1013-1018, March 2011.

[24] H. Kamoda, T. Iwasaki, J. Tsumochi, et al., "60-GHz Electronically Reconfigurable Large Reflectarray Using Single-Bit Phase Shifters," in *IEEE Transactions on Antennas and Propagation*, vol. 59, no. 7, pp. 2524-2531, July 2011.

[25] S. Shahid and G. G. Gentili, "Shaped horn antenna for spot focusing THz imaging application," *2016 Loughborough Antennas & Propagation Conference (LAPC),* Loughborough, 2016, pp. 1-4.

[26] E. Danieli and Y. Pinhasi, "Variable focusing antenna for wireless power transmission and remote sensing at millimeter wavelengths," *2012 IEEE 27th Convention of Electrical and Electronics Engineers in Israel*, Eilat, 2012, pp. 1-1.

[27] G. P. Le Sage, "3D Printed Waveguide Slot Array Antennas," in *IEEE Access*, vol. 4, pp. 1258-1265, 2016.

[28] E. Gandini, A. Tamminen, A. Luukanen, et al., "Wide Field of View Inversely Magnified Dual-Lens for Near-Field Submillimeter Wavelength Imagers," in IE*EE Transactions on Antennas and Propagation*, vol. 66, no. 2, pp. 541-549, Feb. 2018.

[29] L. Shafai, A. A. Kishk, and Sebak, "Near field focusing of apertures and reflector antennas," in *Proc. IEEE Communications, Power and Computing Conf.*, May 22–23, 1997, pp. 246–251.

[30] I. Dierking. [Online]. Available: https://en.wikipedia.org/wiki/File:Food_Polarization-Dierking.jpg. [Accessed 09 2020].

[31] H. Legay and L. Shafai, "New stacked microstrip antenna with large bandwidth and high gain," *Inst. Elect. Eng. Proc. Microw. Antennas Propagation*, vol. 141, no. 3, pp. 199–204, Jun. 1994.

[32] P. Juyal, L. Shafai, "Sidelobe Reduction of TM12 Mode of Circular Patch via Non-resonant Narrow Slot", *IEEE Trans. Antennas Propagation*, vol. 64, pp. 3361-3369, 2016.

[33] A. Vosoogh and P.-S. Kildal, "Simple formula for aperture efficiency reduction due to grating lobes in planar phased arrays," *IEEE Trans. Antennas Propagation*, vol. 64, no. 6, pp. 2263–2269, Jun. 2016.

[34] K. C. Kerby and J. T. Bernhard, "Sidelobe level and wideband behavior of arrays of random subarrays," *IEEE Trans. Antennas Propagation*, vol. 54, no. 8, pp. 2253–2262, Aug. 2006.

[35] S. A. Razavi et al., "2x2-Slot Element for 60-GHz Planar Array Antenna Realized on Two Doubled-Sided PCBs Using SIW Cavity and EBG-Type Soft Surface fed by Microstrip-Ridge Gap Waveguide," in *IEEE Transactions on Antennas and Propagation*, Sept. 2014.

[36] G. Mayhew-Ridgers et al., "Accuracy of the gain-transfer method for a standard gain antenna and a test antenna with equal aperture dimensions," *C COMSIG '98. Proceedings of the 1998 South African Symposium on*, Rondebosch, 1998.

[37] Olimex, "A13-olinuxino-micro user manual." https://www.olimex. com/Products/OLinuXino/A13/ A13-OLinuXino-MICRO/open-sourcehardware, accessed April 3, 2016.

[38] (2019). Trusthub. [Online]. Available: http://www.trusthub.org/benchmarks/trojan.

[39] K. Pokovic, T. Schmid and N. Kuster, "Millimeter-resolution E-field probe for isotropic measurement in lossy media between 100 MHz and 20 GHz," in *IEEE Transactions on Instrumentation and Measurement*, vol. 49, no. 4, pp. 873-878, Aug. 2000.

[40] M. Wu and M. Chuang, "Application of Transmission-Line Model to Dual-Band Stepped Monopole Antenna Designing," in *IEEE Antennas and Wireless Propagation Letters*, vol. 10, pp. 1449-1452, 2011.

[41] Govindanarayanan, Idayachandran, and Rangaswamy, Nakkeeran, "A Broadband Stepped Monopole Antenna with Loop Ground", *Wireless Personal Communications*, vol. 96, no. 3, pp. 4251-4261, Oct. 2017.

[42] (2019). Zaber. [Online]. Available:https://www.zaber.com/products/linear-stages/X-LSQ-E/details/X-LSQ150A-E01/documents.

[43] N. Llombart, K. B. Cooper, R. J. Dengler, T. Bryllert and P. H. Siegel, "Confocal Ellipsoidal Reflector System for a Mechanically Scanned Active Terahertz Imager," in *IEEE Transactions on Antennas and Propagation*, vol. 58, no. 6, pp. 1834-1841, June 2010.

[44] P. -. Kildal and M. M. Davis, "Characterisation of near-field focusing with application to low altitude beam focusing of the Arecibo tri-reflector system," in *IEEE Proceedings - Microwaves, Antennas and Propagation*, vol. 143, no. 4, pp. 284-292, Aug. 1996.

[45] R. C. Hansen, "Focal region characteristics of focused array antennas," *IEEE Trans. Antennas Propag*., vol. 33, no. 12, pp. 1328–1337, Dec. 1985.

[46] T. Milligan and J. Wiley, Modern Antenna Design. New York NY, USA: Wiley Online Library, 2005.

[47] B. E. A. Saleh, M. C. Teich, Fundamentals of Photonics, New York: Wiley, 1991.

[48] CST, Darmstadt, Germany, 2017. Available: https://www.cst.com/.

[49] [Online]. Available: https://www.ultra-herley.com /uploads/herley/datasheets /cti/Ultra%20Herley%20Series% 20PDRO.pdf.

[50] [Online]. Available: http://www.nordengroup.com /product-group /frequency-multiplier- 33-to-50-ghz/.

[51] [Online]. Available: http://www.vadiodes.com /en/wr6-5x3.

[52] [Online]. Available: http://vadiodes.com /en /wr2-8shm.

[53] S. Kim and A. G. Zajić, "Statistical Characterization of 300-GHz Propagation on a Desktop," in *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3330-3338, Aug. 2015.

[54] E. Gandini, A. Tamminen, A. Luukanen and N. Llombart, "Wide Field of View Inversely Magnified Dual-Lens for Near-Field Submillimeter Wavelength Imagers," in *IEEE Transactions on Antennas and Propagation*, vol. 66, no. 2, pp. 541-549, Feb. 2018.

[55] J. Ruze, "Antenna tolerance theory—A review," in *Proceedings of the IEEE*, vol. 54, no. 4, pp. 633-640, April 1966..

[56] C.-B. Juang, L. Finzi, and C. J. Bustamante, "Design and application of a computer-controlled confocal scanning differential polarization microscope," *Rev. Sci. Instrum*., vol. 59, no. 11, pp. 2399–2408, 1988.

[57] C. Ciano et al., "Confocal Imaging at 0.3 THz With Depth Resolution of a Painted Wood Artwork for the Identification of Buried Thin Metal Foils," in *IEEE Transactions on Terahertz Science and Technology*, vol. 8, no. 4, pp. 390-396, July 2018.

[58] Virginia Diodes, Nominal Horn Specifications. [Online]. Available: https://www.vadiodes.com/images/AppNotes/VDI_Feedhorn_Summary_2020.05.04.pdf.

[59] (2020). Zaber. [Online]. Available:https://www.zaber.com/products/linear-stages/X-LSQ-E/details/X-LSQ150A-E01/documents.

[60] [Online]. Available: https://www.ultra-herley.com /uploads/herley/datasheets /cti/Ultra%20Herley%20Series% 20PDRO.pdf.

[61] P. Juyal, S. Adibelli, N. Sehatbakhsh and A. Zajic, "A Directive Antenna Based on Conducting Disks for Detecting Unintentional EM Emissions at Large Distances," in *IEEE Transactions on Antennas and Propagation*, vol. 66, no. 12, pp. 6751-6761, Dec. 2018.

[62] S. Adibelli, P. Juyal, L. N. Nguyen, M. Prvulovic, and A. Zajic, "Near Field Backscattering for Hardware Trojan Detection ," in *IEEE Transactions on Antennas and Propagation, June 2020*.

[63] S. Adibelli, P. Juyal, C. Cheng and A. Zajic, "Terahertz Near-Field Focusing Using a 3-D Printed Cassegrain Configuration for Backscattered Side-Channel Detection," in *IEEE Transactions on Antennas and Propagation*, Oct. 2019.

[64] S. Adibelli, P. Juyal, , M. Prvulovic, and A. Zajic, "THz Backscatter Side-Channel Sensing at a Distance“, Submitted to *IEEE Transactions on Antennas and Propagation*.